FACULDADE DE DIREITO DE VITÓRIA
CURSO DE GRADUAÇÃO EM DIREITO

VANESSA CAMARA CAMPOS LESSA

O uso de algoritmos pelas redes sociais e suas consequências: uma análise a luz da Lei Geral de Proteção de Dados Pessoais e da modulação deleuziana

VITÓRIA
2022.1

VANESSA CAMARA CAMPOS LESSA

O uso de algoritmos pelas redes sociais e suas consequências: uma análise a luz da Lei Geral de Proteção de Dados Pessoais e da modulação deleuziana

Monografia apresentada ao Curso de Graduação em Direito da Faculdade de Direito de Vitória, como requisito parcial para obtenção do grau de bacharel em Direito.

Orientador: Prof. Dr. Paulo Neves Soto

VITÓRIA

2022.1

VANESSA CAMARA CAMPOS LESSA

O uso de algoritmos pelas redes sociais e suas consequências: uma análise a luz da Lei Geral de Proteção de Dados Pessoais e da modulação deleuziana

Monografia apresentada ao Curso de Graduação em Direito da Faculdade de Direito de Vitória, como requisito parcial para obtenção do grau de bacharel em Direito.

Orientador: Prof. Paulo Neves Soto

Aprovada em _____ de _____ de 2022.

COMISSÃO EXAMINADORA

Profº. Drº. Paulo Neves Soto
Faculdade de Direito de Vitória
Orientador

_____

AGRADECIMENTOS

Aos meus pais, por sempre me apoiarem, me fazerem acreditar que é possível e por toda a ajuda que me proporcionaram para que este Trabalho de Conclusão de Curso fosse feito da melhor forma, com calma e persistência.

Ao meu namorado por todo o suporte e compreensão quanto aos meus horários dedicados aos estudos e principalmente a este Trabalho de Conclusão de Curso e por me ouvir nos momentos de crise.

Ao meu orientador, por todo o auxílio durante a escrita deste Trabalho de Conclusão de Curso, por me fazer refletir mais sobre o tema e por todas as indicações que contribuíram para que esta pesquisa fosse realizada e para o aperfeiçoamento do texto.

“Minha ilusão de livre-arbítrio provavelmente vai se desintegrar à medida que eu me deparar, diariamente, com instituições, corporações e agências do governo que compreendem e manipulam o que era, até então meu inacessível reino interior.”

Yuval Noah Harari

RESUMO

Diante do desenvolvimento das tecnologias da informação e da comunicação os algoritmos foram introduzidos nesse contexto como mecanismo fundamental para selecionar as informações mais relevantes, identificar padrões de comportamentos e predizer as ações futuras. A presente pesquisa consiste em analisar o uso de algoritmos pelas redes sociais e suas consequências, o que se justifica em razão da presença do aumento do uso desses códigos nas plataformas digitais, principalmente para auxiliar na publicidade direcionada. O objetivo desse estudo é verificar a previsão abstrata e prática da LGPD, com a finalidade de identificar se há violação ao princípio da transparência e, consequentemente, se existe uma modulação deleuziana na sociedade brasileira, para tanto utilizou-se do método dialético. A pesquisa dividiu-se em três capítulos, nos quais tratou-se de apresentar o contexto da sociedade da informação e da sociedade de controle, a evolução do regime jurídico aplicado a proteção de dados e, por fim, a utilização dos algoritmos pelas redes sociais e suas consequências. Diante disso, concluiu-se que o princípio da transparência não é respeitado devido a falha no consentimento, bem como, que existe a modulação algorítmica na sociedade brasileira em razão da formação de perfis e da vigilância ubíqua.

Palavras-chave: Algoritmos; Redes sociais; Proteção de Dados; Princípio da Transparência; Modulação Deleuziana.

ABSTRACT

In front of information and communication technologies development, the algorithms have been introduced in this context as a fundamental mechanism to select the most relevant information, identify behavior patterns, and predict future actions. This research consists of analyzing the use of algorithms by social media and their consequences, which is justified by the presence of increased use of theses codes on digital plataforms, mainly to help targeted advertising. The aim of this study is to check the abstract and pratical legal prediction of LGPD, in order to identify wether there is a violation of the transparency principle and, consequently, wether there is a deleuzian modulation in brazilian society, for that, the dialectical method was used. The research was divided in three chapters, in which it was presented the context of the information society and the control society, the evolution of legal rules applied to data protection and, finally, the use of algorithms by social media and their consequences. Therefore, it was conclued that the transparency principle is not respected due to the failure to consent, as well as that there is algorithmic modulation in brazilian society because of the profiling and ubiquitous surveillance.

Key words: Algorithms; Social media; Data Protection; Transparency Principle; Deleuzian Modulation.

SUMÁRIO

INTRODUÇÃO

Em razão do surgimento das tecnologias da informação e da comunicação, percebe-se uma maior circulação de informação, a qual passou a ser de extrema importância para a sociedade, uma vez que consegue circular em escala global. Diante disso, nota-se a formação da sociedade da informação, a qual se desenvolve por meio da informação e dos dados. De igual modo, ante a presença constante das tecnologias da informação no cotidiano dos indivíduos tem-se a sociedade de controle, a qual se caracteriza pelo monitoramento frequente dos indivíduos por intermédio dos aparelhos digitais.

Essa sociedade tem como elemento principal para a produção de riquezas a informação. Nesse sentido, foi inserido nas tecnologias da informação os algoritmos, os quais são capazes de, utilizando-se dos dados pessoais, identificar padrões de comportamento dos indivíduos e predizer suas ações futuras. Assim, esses códigos foram inseridos na Internet e nas redes sociais a fim de auxiliar no direcionamento do conteúdo aos usuários como forma de impulsionar a economia.

Para que os algoritmos atinjam seu objetivo é necessário realizar a coleta de dados pessoais, os quais irão servir de parâmetro para a análise e a previsão do comportamento. Ocorre que, tal prática sem o devido cuidado pode provocar lesão ao indivíduo titular dos dados, como à sua privacidade. Nesse contexto, surgiram normas para regulamentar o uso dos dados pessoais, como a coleta, o tratamento, o armazenamento e o compartilhamento, bem como proteger o titular dos dados.

No Brasil, foi promulgada em 2018 a Lei nº 13.709, Lei Geral de Proteção de Dados Pessoais (LGPD), a qual tem como objetivo proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural. A LGPD (BRASIL, 2018) procura tratar de modo específico sobre a proteção de dados no Brasil, trazendo normas que conferem validade ao tratamento dos dados, assim como fundamentos e princípios a serem observados.

Diante disso, esta pesquisa tem como tema o uso de algoritmos pelas redes sociais no Brasil e suas consequências. Assim, desenvolveu-se a partir do seguinte questionamento: é possível identificar se há violação ao princípio da transparência, previsto no art. 6º, IV da LGPD (BRASIL, 2018) e, consequentemente, a presença da modulação deleuziana na sociedade brasileira, ante a utilização de algoritmos pelas redes sociais?

O estudo e a compreensão do tema se fazem necessários tendo em vista que a LGPD (BRASIL, 2018) entrou em vigor completamente em 2021. Portanto, observa-se um grande movimento das empresas para se adequarem a Lei (BRASIL, 2018), no entanto, não se visualiza o mesmo quando se trata das redes sociais no Brasil. Assim, importante compreender se, quando há o uso de algoritmos pelas redes sociais no âmbito brasileiro, a LGPD (BRASIL, 2018) está sendo observada ou se há lesão aos direitos fundamentais do titular dos dados.

Ademais, a pesquisa se mostra importante na medida em que busca analisar se há um controle social operado pelos algoritmos, que a partir da criação de perfis direcionam publicidade e conteúdos relacionados as preferências e interesses do usuário. Desse modo, diante da presença constante dos aparelhos digitais no cotidiano dos indivíduos, importante identificar se tais aparelhos exercem um controle sobre os indivíduos, bem como se o direcionamento de conteúdos é prejudicial para a sociedade.

Nesse contexto, a pesquisa tem como objetivos analisar a previsão abstrata da LGPD (BRASIL, 2018) e verificar como essa se concretiza na prática, com a intenção de desenvolver uma reflexão sobre uma possível violação ao princípio da transparência, bem como sobre a possível existência de uma modulação deleuziana na sociedade brasileira. Para isso, será utilizado o método dialético, o qual se caracteriza pelo uso da discussão ao propor uma tese e contrapô-la com uma tese contrária, e, ao final construir uma síntese decorrente dessa contraposição.

Com a intenção de alcançar o objetivo proposto, esse trabalho foi estruturado em três capítulos, cada um deles dividido em seções. De modo geral, buscou-se apresentar o cenário no qual se encontram os algoritmos e os dados pessoais, em seguida o regime

jurídico no qual estão inseridos, e por fim, tratar sobre as consequências do uso dos algoritmos pelas redes sociais.

No primeiro capítulo será apresentada a sociedade da informação e a sociedade de controle e seus respetivos elementos. Assim, será demonstrado quando surgiram e como podem ser identificadas, destacando-se a presença da Internet, das redes sociais, dos algoritmos, do *Big Data*, da vigilância ubíqua, da bolha dos filtros e da modulação deleuziana.

No segundo capítulo será retratado a evolução do regime jurídico referente a proteção de dados pessoais, no qual discorrerá sobre a legislação europeia e sobre a legislação brasileira. Será demonstrado como se iniciou a previsão legislativa sobre o tema no âmbito europeu e, no contexto nacional, será exposto como era regulamentado o tema no ordenamento jurídico antes do advento da Lei Geral de Proteção de Dados Pessoais (BRASIL, 2018), como se encontra disciplinado na LGPD (BRASIL, 2018) e, também, serão abordados alguns Projetos de Lei apresentados ao Congresso Nacional entre 2019 e 2021.

No terceiro capítulo, por fim, serão analisadas as possíveis consequências do uso de algoritmos pelas redes sociais. Assim, será tratado, em específico, sobre a hipótese legal do consentimento, previsto na LGPD (BRASIL, 2018) e, sobre a formação de perfis e as decisões automatizadas ocorridas nas redes sociais.

1 ASPECTOS SOCIAIS DA TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

A fim de compreender sobre a utilização de algoritmos nas redes sociais importante apresentar o contexto social na qual estes estão incluídos. Assim, inicialmente será tratado sobre a Sociedade da Informação, explicando o que vem a ser esse tipo de organização social, a partir de quando ela começou a ser identificada na sociedade e apresentando seus elementos constitutivos. Em um segundo momento, será

discorrido sobre a Sociedade de Controle, como ela se estrutura e quais são os elementos que a caracterizam.

1.1 A SOCIEDADE DA INFORMAÇÃO

A expressão “Sociedade da Informação” surgiu em 1993, ao ser utilizada pelo Presidente da Comissão Europeia, Jacques Delors, durante o Conselho Europeu, em seu discurso no qual tratava sobre a infraestrutura da informação (SARTORI; BAHIA, 2019, p. 230). A sociedade da informação, de acordo com Paulo Hamilton Siqueira Júnior (2007, p. 2),

> é constituída em tecnologias de informação e comunicação que envolve a aquisição, o armazenamento, o processamento e a distribuição da informação por meios eletrônicos, como rádio, televisão, telefone e computadores, entre outros. Essas tecnologias não transformam a sociedade por si só, mas são utilizadas pelas pessoas em seus contextos sociais, econômicos e políticos, criando uma nova estrutura social, em que tem reflexos na sociedade local e global, surgindo assim a sociedade da informação.

A sociedade da informação desenvolveu-se a partir da década de 80, sendo consequência da revolução tecnológica, pela qual obteve-se uma sociedade pautada na informação. Corresponde, assim, a uma sociedade a qual se desenvolve por meio de informações e dados (SIQUEIRA JÚNIOR, 2007). Nesse sentido, “o termo sociedade da informação designa a sociedade marcada pelo avanço tecnológico no tratamento da informação” (SIQUEIRA JÚNIOR, 2007, p. 2).

Manuel Castells (2011. p. 108 - 109) caracteriza essa sociedade com base em alguns aspectos, primeiro considera que a informação é sua matéria-prima, sendo aplicável a tecnologia sobre a informação e não apenas informação na tecnologia, em segundo entende que a informação integra a vida humana, assim, tudo referente a existência humana é moldado pelo meio tecnológico, em terceiro, afirma que a sociedade da informação é constituída em rede, e, em razão de sua configuração topológica e das novas tecnologias da informação, pode ser inserida em qualquer tipo de processo ou organização, em quarto e quinto, indica que esta é baseada na flexibilidade e na integração, ou seja, os processos presentes na sociedade da informação são

reversíveis, podendo ser modificados e reconfigurados, ante a sua alta fluidez, além disso seus sistemas são todos integrados entre si, não sendo possível distingui-los.

Nesse contexto, Bruno Ricardo Bioni (2021, p. 3) afirma que “a sociedade, ao longo do tempo, sofreu diversas formas de organização social”, possuindo, em cada uma delas, um elemento caracterizador daquela sociedade, o qual possibilita o reconhecimento e a distinção de cada período histórico. Desse modo, a sociedade atual,

> está encravada por uma nova forma de organização em que a informação é o elemento nuclear para o desenvolvimento da economia, substituindo os recursos que outrora estruturavam as sociedades agrícolas, industrial e pós-industrial (BIONI, 2021, p. 4).

A informação e o conhecimento são os valores principais atribuídos a sociedade da informação (SIQUEIRA JÚNIOR, 2009, p. 218). Desse modo, a informação consiste no elemento central da sociedade e serve como adjetivo para sua denominação. Isso porque a sociedade passou a se organizar e construir sua estrutura com base nesse novo elemento, a informação, assim como, “as máquinas a vapor e a eletricidade, bem como os serviços, respectivamente, nas sociedades agrícola, industrial e pós-industrial” (BIONI, 2021, p. 5).

No Brasil, o termo ‘Sociedade da Informação’ foi pioneiramente tratado por Tadao Takahashi (2000) no Livro Verde, o qual abrange diversas ações com o objetivo de unir governo e sociedade para impulsionar a sociedade da informação no Brasil. Na obra, o referido autor, traduz o termo como “uma nova era em que a informação flui a velocidade e em quantidades há apenas poucos anos inimagináveis, assumindo valores sociais e econômicos fundamentais” (TAKAHASHI, 2000, p. 3). Sob essa perspectiva, Paulo Hamilton Siqueira Júnior (2007, p. 2), assevera que,

> A expressão sociedade da informação designa uma forma nova de organização da economia e da sociedade. O fator diferencial da sociedade da informação é que cada pessoa e organização não só dispõem de meios próprios para armazenar conhecimento, mas também têm uma capacidade quase ilimitada para acessar a informação gerada pelos demais e potencial para ser um gerador de informação para outros.

Assim, pode-se dizer que a sociedade da informação se molda a partir das informações, do armazenamento de conhecimento e dados, e, consequentemente do tratamento destes. O conceito de sociedade da informação não se limita ao aspecto tecnológico, engloba também o tratamento e a transmissão de informações, ou seja, é definida pela circulação de informações às quais é atribuído valor econômico.

> Uma nova mercadoria gera uma indústria lucrativa e de rápido crescimento, levando os reguladores antitruste a intervir a fim de restringir aqueles que controlam o fluxo. Há um século, o recurso em questão era o petróleo. Agora, preocupações semelhantes estão sendo levantadas pelos gigantes que lidam com dados, o petróleo da era digital (THE ECONOMIST, 2017).

Nesse sentido, conforme dito em 2006 pelo matemático britânico Clive Humby "*Data is the new oil*"[1], uma vez que "assim como o petróleo precisa ser refinado, dados precisam ser analisados" (RIPARI, 2019), de modo que não basta seu estado "bruto", para que os dados tenham valor eles devem passar pelo processo de tratamento, o qual se assemelha ao processo de refinamento do petróleo. Portanto, "nessa era, a informação transforma-se em fonte de valor e poder. A informação e o conhecimento são fontes de riqueza" (SIQUEIRA JÚNIOR, 2007, p. 5).

> Seguindo esse raciocínio, é seguro afirmar que a maior riqueza se encontra não nos dados em si, mas sim na capacidade de usá-los de forma analítica. A inteligência por trás deles é quem determina seu maior valor pois, a partir dela, serão extraídas as descobertas capazes de transformar a realidade não só das organizações, mas de diferentes mercados (RIPARI, 2019).

Bruno Ricardo Bioni (2021, p. 5) expõe que "a computação eletrônica e a Internet são as ferramentas de destaque" dessa nova organização social. A Internet permite uma grande circulação de informações e dados em uma proporção mundial (MARTELETO, 2010, p. 32), constituindo o meio de comunicação universal da sociedade da informação (CASTELLS, 2011, p. 433).

Segundo Cláudio de Oliveira Santos Colnago (2016, p. 171) "a Internet contribui para o desenvolvimento político, econômico e social, permitindo uma sociedade mais bem informada e capaz de fazer sua voz ser ouvida de maneira muito mais eficaz do que antes do seu advento". No mesmo sentido, Bruno Costa Teixeira (2012, p. 42) afirma

[1] Os dados são o novo petróleo.

que “a Internet é o sustentáculo tecnológico que permite e fomenta” a formação das redes na sociedade da informação.

> A popularização da Internet no Brasil e no mundo – ainda que incompleta, mas crescente, no primeiro – conduz a Sociedade a um estágio diferenciado de comunicação e interação. Já não se fala mais em “grande rede mundial de computadores”, uma vez que a *web* mais parece uma grande rede mundial de pessoas. “Nós somos a *web*” e, a cada dia que passa, isso fica mais evidente para o grande número de pessoas que usam a rede (TEIXEIRA, 2012, p. 41).

No ordenamento jurídico brasileiro encontra-se o conceito de Internet estabelecido pela Lei n. 12.965/2014 - Marco Civil da Internet (BRASIL, 2014), em seu art. 5º, I, o qual dispõe ser a Internet um “sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para o uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes”.

A Internet consiste em um “mecanismo de interação pessoal e doméstica” (GARCIA, J., 2020), formada por uma “plataforma que conecta as pessoas e aquilo que elas produzem em forma de dados” (GARCIA, J., 2020). Nesse sentido, Regina Maria Marteleto (2010, p. 32) afirma que,

> A Internet, chamada “redes das redes”, caracteriza-se por dois aspectos principais. Primeiro, é um grande acervo de dados e de informações aberto a múltiplas escritas, consultas, leituras, usos e apropriações. Segundo, é uma arena ampliada geograficamente e socialmente para interação, comunicação e sociabilidade. Portanto, atua como suporte de atividades cooperativas em escala mundial, organizadas no âmbito de comunidades massivamente interativas como *Wikipedia*, os coletivos de desenvolvedores de *softwares* livres, os *blogs*, os jogadores em rede ou as plataformas relacionais, como *Facebook, MySpace*, etc.

Nesse contexto, encontram-se as redes sociais, as quais “constituem uma das estratégias subjacentes utilizadas pela sociedade para o compartilhamento da informação e do conhecimento, mediante as relações entre atores que as integram” (TOMAÉL; ALCARÁ; DI CHIARA, 2005, p. 93). As redes sociais constituem um meio utilizado pela sociedade para compartilhar informações e conhecimento na Internet, “a maioria das tecnologias de mídia social surgiram antes de 2005, quando Tim O’Reilly estabeleceu o conceito de web 2.0” (FUCHS, 2014, p.48, tradução nossa), se tornando realmente populares a partir de 2010 (FUCHS, 2014, p. 48).

Christian Fuchs (2014, p. 49, tradução nossa) ao questionar o que seria a mídia social conclui que “é um sistema tecno-social no qual estruturas tecnológicas interagem com relações sociais e atividades humanas de modo complexo”. Regina Maria Marteleto (2001, p. 72), afirma de forma detalhada que as redes sociais são “um conjunto de participantes autônomos, unindo ideias e recursos em torno de valores e interesses compartilhados”. Em um cenário carregado de novas tecnologias, possibilitou-se que os meios de comunicação criassem formas mais interativas de transmitir as informações, expandindo os limites espaciais e temporais e, consequentemente, permitindo que a comunicação pudesse acontecer a qualquer momento (VERMELHO; VELHO; BONKOVOSKI; PIROLA, 2014, p. 182).

A expressão ‘redes sociais’ assemelha-se a tecnologia da informação e comunicação, atualmente, é um termo utilizado por diversas áreas (VERMELHO; VELHO; BONKOVOSKI; PIROLA, 2014, p. 183) e que oferece infinitos significados, sendo aplicado na comunicação como, rede social digital, mídia social, mídia digital e outros (VERMELHO; VELHO; BONKOVOSKI; PIROLA, 2014, p. 183). Desse modo, os autores Sônia Cristina Vermelho, Ana Paula Machado Velho, Amanda Bonkovoski e Alisson Pirola (2014, p. 188), após reunirem diferentes conceitos existentes sobre as redes sociais, concluíram pela formulação de um conceito de rede social digital, como sendo,

> A macroestrutura tecnológica que dá suporte a um conjunto de atores sociais (sujeito e instituições) conectadas por *laços sociais* (BATISTA, 2012; RAHME, 2010; FREUD, 1976, 1997), os quais são formados, mantidos e reforçados (ou não) por meio de *interações sociais* (VYGOTSCKY, 1989, 1987; BAKHTIN, 988; LURIA, 1987). As interações são concretizadas, realizadas dentro de uma relação de troca de conteúdos. Estes podem ser criados pelas mais diferentes linguagens disponíveis no formato digital: textual, sonora, audiovisual e imagética. Estas ferramentas potencializam a manutenção e a expansão dos laços sociais, além de ajudarem a visualizar as redes de relacionamento das quais cada sujeito faz parte.

Assim, infere-se do conceito de redes sociais a formação de uma sociedade pautada na interação entre os seus integrantes e na criação de vínculos entre eles, o que reforça a capacidade de atuação, de compartilhamento, de aprendizagem, de captação de recursos e de mobilização nesses espaços constituídos na Internet (MARTELETO, 2010, p. 28).

Em meio a grande circulação de dados e informações na Internet, o ambiente virtual igualava-se ao caos, conforme sustenta José Wilson Correa Garcia (2020), o que gerava diversos questionamentos sobre como tornar o espaço mais tranquilo, com menos experiências aleatórias aos usuários. A introdução dos algoritmos na Internet foi a forma encontrada para “transformar o ambiente caótico em uma experiência agradável para o usuário” (GARCIA, J., 2020), pois estes mecanismos seriam capazes de organizar a enorme base de dados existente no mundo virtual (GARCIA, J. 2020). Assim, “os algoritmos foram alterados para criar uma nova experiência de interação do usuário com o que ele procura na internet, intermediado pela lógica quantitativa da identificação” (GARCIA, J., 2020).

As redes sociais, atualmente, também se organizam por algoritmos, os quais definem o que pode ser visto e a quantidade de pessoas que podem visualizar um conteúdo (SILVEIRA, 2019, p. 20). Os algoritmos são, resumidamente, conceituados por Kowalski (1979), como o resultado da soma entre lógica e controle. São representados por códigos matemáticos aplicados a tecnologia e as máquinas, e segundo os programadores virtuais, usando a linguagem de programação, são entendidos como “sequência de passos que resolvem um determinado problema” (GARCIA, J., 2020).

Entretanto, para além do resultado de uma operação matemática e do conceito usado pelos programadores, os algoritmos, segundo Tarleton Gillespie (2014, p. 167, tradução nossa) “desempenham um papel cada vez mais importante na seleção de quais informações são consideradas mais relevantes para nós, um aspecto crucial da nossa participação na vida pública”. Os algoritmos atuam nas operações realizadas pelos usuários na Internet de forma que,

> Mapeiam nossas preferências em relação a outros, trazendo ao nosso encontro sugestões de fragmentos novos ou esquecidos da cultura. Algoritmos gerenciam nossas interações nas redes sociais, destacando as novidades de um amigo enquanto exclui as de outros. (GILLESPIE, 2014, p. 167, tradução nossa).

Ademais, Tarleton Gillespie (2014, p. 167, tradução nossa) declara que “juntos, esses algoritmos não só nos ajudam a encontrar informações, mas também nos fornecem um meio de saber o que há para ser conhecido e como fazê-lo”. Nesse sentido, é o exposto por Sérgio Amadeu da Silveira (2020, p. 68), ao afirmar que,

> Ao canalizar as atenções, o algoritmo atua oferecendo caminhos específicos, direções a se tomar, como um *nudge* (em português, cutucar, empurrar, incentivar), uma suave indicação e uma alteração de comportamento de maneira previsível, sem proibições, sendo uma forma suave de controle por design, tal como o ordenamento dos resultados do mecanismo de busca que oferece nos primeiros resultados os links que tendem a ser mais escolhidos, pela posição que ocupam.

Sob essa perspectiva João Roberto Gorini Gamba (2021), chama tal fenômeno de "arquitetura de escolha", uma vez que os algoritmos, ao serem aplicados as redes sociais, funcionam com o objetivo de "determinar a publicidade e a ordem das publicações apresentadas aos usuários (GAMBA, 2021). Assim, "são utilizados para observar nosso comportamento e nossos interesses, bem como predizer nossas necessidades futuras e nossas ações futuras" (HOFFMANN-RIEM, 2019, p. 126). Nas palavras de Paulo César Castro (2016, p. 27),

> O algoritmo funciona sobre o seguinte princípio básico: input > processamento > output. Após a entrada de algumas informações básicas em um dispositivo, elas são processadas segundo um algoritmo que, ao final apresenta um resultado como saída.

A expansão da sociedade da informação ocasionou a expansão dos computadores e dos *softwares*, além de automatizar as atividades de produção. Assim, "com o avanço das tecnologias da informação e comunicação tornou-se indispensável a utilização de softwares" (SILVEIRA, 2019, p. 17), os quais "são formados por algoritmos" (SILVEIRA, 2020, p. 63 - 64). Desse modo, inseridos no campo da tecnologia da informação e da comunicação os algoritmos operam de modo que,

> Transformam a informação e alguns deles são classificadores. Em contato com um conjunto de dados, os algoritmos selecionam aqueles que foram definidos como úteis para a finalidade a que foram programados. Enquanto certos algoritmos atuam em busca de padrões, outros realizam uma sequência de operações mais simples. [...] algoritmos podem ser determinísticos, probabilísticos, prescritivos, entre outras possibilidades de seu desenvolvimento. Servem como verdadeiros filtros informacionais (SILVEIRA, 2019, p. 20)

Os algoritmos são utilizados pelas redes sociais encontrando padrões no comportamento dos usuários com a finalidade de influenciar suas ações. Eles operam na filtragem das informações dos usuários, criando perfis que sejam compatíveis com o dos destinatários (ROSSETTI; ANGELUCI, 2021 p. 11) e, "contribuem para facilitar

e personalizar a experiência dos usuários (VIDAL JÚNIOR, 2016). Assim, conforme descrevem Bruna Bastos e Luiza Berger von Ende (2020, p. 21),

> Sob diversos formatos essas tecnologias identificam cada usuário conforme sua atividade *online* e criam grandes bases de dados a seu respeito, tornando possível às empresas identificarem os interesses e características de cada pessoa para que a veiculação de anúncios seja especialmente exposta àqueles que a empresa julga serem mais suscetíveis ou adequadas a responder ao produto ou à ideia que veiculam.

No mesmo sentido, Eli Pariser (2012 p. 147) afirma que, “pela primeira vez, um meio é capaz de descobrir quem somos, do que gostamos e o que queremos.”. Os algoritmos, por meio da personalização, se tornam lucrativos, atuando com a publicidade direcionada e a partir de ajustes nos conteúdos que cada usuário recebe nas plataformas digitais (PARISER, 2012, p. 147). Afirma o autor, ainda, que os algoritmos “são mecanismos de previsão que criam e refinam constantemente uma teoria sobre quem somos e sobre o que vamos fazer ou desejar a seguir” (PARISER, 2012, p. 11).

Nota-se, portanto, que os algoritmos são códigos inseridos nas tecnologias da informação e da comunicação, presentes na Internet e também aplicados as redes sociais, os quais rastreiam as atividades dos usuários online reunindo informações e, dessa forma, selecionam os conteúdos adequados para o perfil de cada indivíduo. Assim, tem como objetivo “descobrir padrões e conexões que de outra forma seriam invisíveis e que podem fornecer informações valiosas sobre os usuários que o gerarem” (SILVEIRA, 2019, p. 22).

Em razão do crescimento da sociedade da informação, principalmente, no ambiente virtual, o qual não apresenta limite espacial, há uma grande quantidade de dados em circulação. “O grande volume de informações disponíveis digitalmente é o que se denomina de *Big Data”*, conforme afirma Émilien Vilas Boas Reis e Bruno Torquato de Oliveira Naves (2020, p. 147).

O *Big Data* corresponde a uma metodologia voltada para o processamento e a organização de dados (BIONI, 2021, p. 36). Conforme expõe Fernando Amaral (2016, p. 12), “Big Data é o fenômeno de massificação de elementos de produção e

armazenamento de dados, bem como os processos e tecnologias, para extraí-los e analisá-los". Nesse sentido, segundo Jéffson Menezes de Sousa (2017, p. 39), o Big Data,

> É um grande volume de dados que permite sua coleta, tratamento, armazenamento e reutilização dos dados, inclusive, dados pessoais sendo que a mudança de escala leva a uma mudança de estado. São tantos os dados e de variáveis características que podem não parecer informações pessoais explícitas, mas que, correlacionadas, reordenados ou reidentificados, após os processos de análises com o *big data*, podem facilmente dizer a quem se referem ou levar ao conhecimento de detalhes íntimos da vida de uma pessoa.

Uma forma de se pensar sobre o termo *Big Data* atualmente, seria de modo a enxergá-lo como um trabalho a ser feito em tamanha proporção "para extrair novas ideia e criar novas formas de valor de maneiras que alterem os mercados, as organizações, a relação entre cidadãos e governos, etc." (MAYER-SCHONBERGER; CUKIER, 2013, p. 4). Tal ferramenta pode influenciar no biohackeamento humano, pois "os algoritmos de computação foram moldados pela seleção natural e não tem emoções nem instintos viscerais" (HARARI, 2018, p. 68).

> Sentimentos morais como indignação, culpa ou perdão derivam de mecanismos neurais que evoluíram para permitir cooperação grupal. Todos esses algoritmos bioquímicos foram aprimorados durante milhões de anos de evolução. Se os sentimentos de algum antigo ancestral cometeram um erro, os genes que configuram esses sentimentos não foram passados à geração seguinte (HARARI, 2018, p. 57).

Yuval Noah Harari (2018, p. 66), questiona se ainda há liberdade na sociedade, uma vez que esta encontra-se cada vez mais fundida com a Inteligência Artificial. O autor afirma que quando ocorrer a fusão entre a biotecnologia e a tecnologia da informação, o resultado será algoritmos de *Big Data* aptos a monitorar os sentimentos dos indivíduos, transmitindo a autoridade humana para os computadores (HARARI, 2018, p. 58).

> Quando a autoridade passa de humanos para algoritmos, não podemos mais ver o mundo como o campo de ação de indivíduos autônomos esforçando-se por fazer as escolhas certas. Em vez disso, vamos perceber o universo inteiro como um fluxo de dados, considerar organismos pouco mais que algoritmos bioquímicos e acreditar que a vocação cósmica da humanidade é criar um sistema universal de processamento de dados – e depois fundir-se a ele (HARARI, 2018, p. 66).

O *Big Data*, tratado pelas ferramentas disponíveis na forma de algoritmos, é responsável por armazenar as informações coletadas, formando um banco de dados com quantidade inimaginável, que serão utilizados para diversas finalidades, sendo uma delas as previsões comportamentais. Tem como atuação principal “aplicar a matemática a enormes quantidades de dados a fim de prever possibilidades” (MAYER-SCHONBERGER; CUKIER, 2013, p. 8). Assim, o *Big Data* corresponde ao volume de dados expostos na sociedade da informação e a atividade de predizer o comportamento dos usuários, ou seja, ao conjunto de informações e também a atuação na manipulação ou “predição”, que somente é possível em razão do tratamento realizado por meio de algoritmos.

> O *big data*, contudo, depende da coleta massiva de informações. A regra é sempre “quanto mais, melhor”. Os dados sequer precisam ser relevantes no momento da sua coleta, pois a importância surgirá depois, com o processamento por meio do algoritmo adequado (MENEZES NETO; MORAIS, 2018, p. 1131).

Nesse sentido, o *Big Data* demonstra o quão importantes são os dados e as informações para a nova organização social. Isso porque, em uma sociedade pautada na informação, os dados e as informações são considerados “fontes de riqueza“ (THE ECONOMIST, 2017), pois é a partir da coleta e do tratamento dos dados e, posteriormente, a transformação em informações que se obtém valor (BOTELHO, 2020, p. 197).

Segundo Yuval Noah Harari (2018, p. 60 – 61), ao navegar na Internet, os algoritmos discretamente monitoram as ações dos indivíduos, e coletam informações, sem que os usuários percebam, assim, o potencial desta informação tratada permite a condução e manipulação do mercado, uma vez que essa informação vale bilhões aos que comercializam produtos e serviços na Internet, em um outro nível, muito mais grave, estes mesmos algoritmos podem ser utilizados para a condução da tomada de decisões eleitorais, formação de opinião e controle social – uma sociedade de controle total.

Diante disso, a sociedade da informação representa uma sociedade na qual a informação é considerada objeto de valor (SIQUEIRA JÚNIOR, 2007). Essa sociedade é composta pelos elementos aqui tratados, Internet, Redes Sociais, Algoritmos e o *Big*

Data, que juntos são responsáveis pelo monitoramento dos indivíduos na sociedade. Assim, as tecnologias da informação presentes nessa sociedade atuam na coleta, no armazenamento e no tratamento dos dados, extraindo deles informações as quais serão objeto de análise para a identificação dos usuários.

A presença dos algoritmos na sociedade é o principal fator que auxilia na prática da formação de perfis, pois eles são responsáveis por rastrear as atividades realizadas na Internet e nas redes sociais e mapear as informações mais relevantes identificando as preferências dos indivíduos. Desse modo, possível perceber que a sociedade da informação também é uma sociedade de constante vigilância dos cidadãos, porém, esta deixa de ser um ato de vigiar (FOUCAULT, 1999) e passa a ser um ato de controle (DELEUZE, 1992), na medida em que, pela aplicação dos algoritmos na Internet e nas redes sociais, além de observar as ações de cada um, também é possível fazer previsões de suas próximas ações, o que possibilita o direcionamento dos conteúdos, com base nas preferências dos usuários.

Nesse sentido, pela aplicação dos algoritmos na sociedade da informação, percebe-se a possibilidade da existência de um controle social, visto que tais códigos conseguem, a partir da análise das preferências pessoais, direcionar os conteúdos para cada usuário. Esse assunto será tratado no próximo item, onde será possível entender como se dá o controle social por meio dos algoritmos na sociedade, denominada de Sociedade de Controle.

1.2 A SOCIEDADE DE CONTROLE

A sociedade de controle é compreendida como “a sociedade da tecnologia da informação, dos desenvolvimentos da inteligência artificial, do *machine learning* e, por extensão, do *deep learning*.” (LEITÃO; SOARES, 2020, p. 163). Tais expressões, nas palavras de Elias Jacob de Menezes Neto e José Luis Bolzan de Morais (2018, p. 1136) são “áreas do saber cujo objetivo é criar sistemas computacionais capazes de acumular conhecimento, tomando decisões com base nas suas experiências

anteriores". Essa sociedade, então, compreende uma organização social, na qual uma de suas características é,

> O monitoramento em 360 graus. Não é mais um olhar de alguém lá fora, alguém que pode estreitar o olhar para dentro da sua casa, através do portão, da janela ou da porta. As empresas chamadas de *Big Data*, que recolhem, classificam e mineram nossos dados, tem a possibilidade de serem o *grande irmão* vigilante diante dos nossos dados digitais (LEITÃO; SOARES, 2020, p. 163).

Nesse contexto, em razão da revolução tecnológica e a expansão da Internet, uma nova formação social emergiu, de forma que "a sociedade passou a conviver em rede" (SOUSA; OLIVEIRA, 2020, p. 614). Estando inseridos na sociedade da informação, os indivíduos vivem também em uma sociedade de controle, afetados pela presença constante da tecnologia (SOUSA; OLIVEIRA, 2020, p. 625).

Identifica-se, portanto, a sociedade de controle pelo contexto no qual os indivíduos estão introduzidos, ou seja, pela participação ostensiva das tecnologias da informação no cotidiano destes e pela introdução do controle por meio dos aparelhos digitais. Assim, a sociedade de controle é marcada pela existência do controle que se opera pelas tecnologias da informação.

Quando se fala em controle esse está associado ao poder. Em meados do século XVIII o filósofo e jurista Jeremy Bentham construiu, por meio de cartas, a ideia de uma estrutura de poder na qual "tratava-se de um novo modo de garantir o poder da mente sobre a mente, em um grau nunca antes demonstrado" (BENTHAM, 2008, p. 17), a fim de propor uma inovação ao sistema prisional. Assim, surgiu a estrutura do Panóptico, construída em um formato circular, com uma torre no centro, chamada pelo autor de alojamento do inspetor, a qual se destinava a otimizar a vigilância, uma vez que os indivíduos teriam a sensação de estarem sendo observados o tempo todo (BENTHAM, 2008).

Conforme tratado por Michel Foucault, (1999, p. 224) o efeito mais importante do Panóptico é "induzir no detento um estado consciente e permanente de visibilidade que assegura o funcionamento automático do poder". No mesmo sentido, Byung-Chul Han (2017, p. 63) afirma que "com o auxílio de técnicas refinadas cria-se a ilusão de

uma vigilância permanente", onde a transparência é unilateral e dá fundamento ao mecanismo de poder e domínio.

> O *Panóptico* de Bentham é a figura arquitetural dessa composição. O princípio é conhecido: na periferia uma construção em anel; no centro, uma torre; esta é vazada de largas janelas que se abrem sobre a face interna do anel; a construção periférica é dividida em celas, cada uma atravessando toda a espessura da construção; elas têm duas janelas, uma para o interior, correspondendo às janelas da torre; outra, que dá para o exterior, permite que a luz atravesse a cela de lado a lado (FOUCAULT, 1999, p. 223)

Jeremy Bentham entendeu que tal estrutura seria aplicável a qualquer estabelecimento, cujo espaço fosse mais parecido com um edifício, em que pudessem "manter sob inspeção um certo número de pessoas" (BENTHAM, 2008, p. 19).

> É óbvio que, em todos esses casos, quanto mais constantemente as pessoas a serem inspecionadas estiverem sob a vista das pessoas que devem inspecioná-las, mais perfeitamente o propósito do estabelecimento terá sido alcançado (BENTHAM, 2008, p. 20).

No século XX Michel Foucault tendo como objetivo a análise da atuação do poder sobre os corpos, isto é, do chamado 'biopoder' utilizou-se da ideia proposta por Bentham (2008) para tratar sobre a disciplina. A primeira análise se deu em sua obra Vigiar e Punir (1999), em que tratou sobre a figura do poder disciplinar, o qual consiste em "um poder que, em vez de se apropriar e de retirar, tem como função maior "adestrar"; ou sem dúvida adestrar para retirar e se apropriar ainda mais e melhor" (FOUCAULT, 1999, p. 195). Segundo Leandro Chevitarese e Rosa Maria Leite Ribeiro Pedro (2005), "o nível de exercício do poder tem como objetivo uma espécie de 'treinamento' dos corpos, através da disciplina".

Gilles Deleuze deu continuidade aos estudos de Michel Foucault sobre o biopoder, no que desenvolveu também uma concepção sobre o controle, e junto com Félix Guattari entre os anos de 1995 e 1997 idealizou uma nova forma de sociedade, a qual estava conectada ao avanço da tecnologia (CHEVITARESE; PEDRO; 2005) e da presença do controle. Assim, o autor afirma que,

> O marketing é agora o instrumento de controle social, e forma a raça impudente de nossos senhores. O controle é de curto prazo e de rotação rápida, mas também contínuo e ilimitado, ao passo a disciplina era de longa duração, infinita e descontínua (DELEUZE, 1992, p. 224).

Nas sociedades disciplinares, a vigilância, como instrumento de fiscalização, operava de forma autoritária, “educando” o comportamento dos indivíduos com base nas consequências disciplinares decorrentes da desobediência (RUIZ, 2004, p. 80). Entretanto, com as tecnologias da informação e do conhecimento, insere-se na sociedade contemporânea novas condições, que modificam a forma de operação do controle, as quais não harmonizam com a sociedade disciplinar, fazendo com que o poder não consiga mais ser exercido por meio da disciplina (RUIZ, 2004, p. 89 - 90).

Assim, novas formas de controle estão surgindo, conforme afirma Gilles Deleuze (1992, p. 216) “estamos entrando nas sociedades de controle, que funcionam não mais por confinamento, mas por controle contínuo e comunicação instantânea”. Portanto, a sociedade de controle substitui a sociedade disciplinar, modificando a estrutura que opera o poder sobre a sociedade.

> A distinção entre interior e exterior, necessária para o pleno funcionamento do modelo pan-ópito, é incapaz de absorver a natureza descentralizada das redes de poder típicas da sociedade em rede, o que demanda uma nova forma de pensar as novas tecnologias de informação e comunicação (TICs) (MENEZES, NETO; MORAIS, 2018, p. 1144 – 1145).

A sociedade de controle relaciona-se com a sociedade disciplinar, no sentido de que ambas tratam da vigilância (SOUSA; OLIVEIRA, 2020, p. 634). Na sociedade disciplinar a vigilância versa sobre o confinamento, enquanto na sociedade de controle a vigilância se volta para as informações que circulam na sociedade e aos indivíduos que as acessam (COSTA, 2004, p. 163 - 164). A vigilância, na sociedade disciplinar, se restringia aos espaços internos, na sociedade de controle ela se expande, em razão das tecnologias da informação, a vigilância consegue atingir todos os espaços, não se limitando mais ao ambiente interno (CHEVITARESE; PEDRO, 2005).

Nesse contexto, Byung-Chul Han (2017, p. 63) entende que no panóptico de Bentham os indivíduos têm ciência de que estão sob constante observação de um vigia, ao contrário, na sociedade de controle, chamada pelo autor de panóptico digital, os indivíduos têm a ilusão de estarem em total liberdade, uma vez que estando conectados em rede, os usuários, reféns de uma excessiva comunicação, contribuem

para a transparência, ao se expor por vontade própria e não mais por uma coação externa.

Por outro lado, há uma diferença fundamental entre a sociedade disciplinar e a sociedade de controle, a qual refere-se à possibilidade de identificar a motivação dos indivíduos.

> Os dispositivos de poder da sociedade disciplinar investem no adestramento compulsivo do indivíduo. O seu objetivo é fabricar um indivíduo treinado nas habilidades requeridas pelas instituições em questão. [...]. O controle, enquanto dispositivo de poder não visa o treinamento do corpo, o disciplinamento do espaço ou a racionalização do tempo; estes, de alguma forma, são requisitos prévios. Os dispositivos de poder do controle têm como alvo a motivação do indivíduo (RUIZ, 2004, p. 88 – 90).

Nesse sentido, Jéffson Menezes de Sousa e Liziane Paixão Silva Oliveira (2020, p. 634) concluem que, a partir da modificação da sociedade disciplinar para a sociedade de controle identifica-se uma mudança nos mecanismos de controle, operado na sociedade disciplinar por meio da estrutura do Panóptico, e na sociedade de controle, pelos bancos de dados automatizados.

Gilles Deleuze (1992) afirma que na sociedade disciplinar o indivíduo é identificado por uma assinatura e um número de matrícula, por outro lado na sociedade de controle são identificados pelo que o autor chama de “cifra”, que nada mais é que uma senha, “os indivíduos tornaram-se ‘dividuais’, divisíveis, e as massas tornaram-se amostras, dados, mercados ou bancos” (DELEUZE, 1992, p. 222). A identificação dos indivíduos como dados, na sociedade de controle, configura um dispositivo de poder importante nessa sociedade, sendo instrumento fundamental para operação do controle.

Essa capacidade de dirigir a motivação dos indivíduos só é possível em razão da vigilância ubíqua presente na sociedade de controle, a qual se refere à quando,

> As atividades dos sujeitos se tornam mediadas pela presença de aparatos digitais durante todo o tempo, isso resulta em uma exploração ubíqua, pois de sua atividade se extrai valor ininterruptamente, e isso acelera a exploração e intensifica o controle (ANTUNES; MAIA, 2018, p. 196).

A vigilância ubíqua corresponde a “onipresença do ambiente virtual” (BIONI, 2021, p. 85), ou seja, o sujeito na sociedade de controle, se encontra rodeado de aparelhos

digitais os quais estão 24 horas conectados à Internet. Assim, como o próprio termo diz, trata-se de uma vigilância que está em toda parte, é onipresente. Na sociedade disciplinar, a vigilância era limitada as escolas, hospitais, prisões, ou seja, ambientes internos. Já na sociedade de controle, devido a presença dos mecanismos de tecnologia da informação e, principalmente, da Internet, a vigilância atravessa os limites espaciais e se manifesta em qualquer lugar, a qualquer momento.

Atualmente, tal cenário é chamado de Internet das Coisas, em que qualquer aparelho está conectado por um sistema de radiofrequência (BIONI, 2021, p. 85). Bruno Ricardo Bioni (2021, p. 86), afirma que essa realidade auxilia e permite continuidade a ideia de vigilância, que era “antes tomada e associada a partir do histórico de navegação e os rastros deixados no mundo *on-line*, agora é transposta para o mundo físico por meio das coisas e objetos presentes no cotidiano do ser humano”.

Segundo Byung-Chul Han (2017, p. 67) “hoje, o globo como um todo está se transformando em um único panóptico. Não existe um fora do panóptico; ele se torna total, não existindo muralha que possa separar o interior do exterior”. A supervisão não ocorre mais com a restrição da liberdade, mas sim a partir da exposição exercida livremente pelos indivíduos, o que contribui para a formação do panóptico digital (HAN, 2017).

Nesse contexto, Eli Pariser (2012, p. 130) ao tratar sobre a bolha dos filtros, afirma que, “os dias nos quais a bolha dos filtros desaparece quando nos afastamos do computador estão contatos”. Isso porque, atualmente, não é necessário estar diante de um computador para que estejamos submetidos a vigilância ubíqua, os aparelhos digitais se desenvolveram e estão presentes cotidianamente, como por exemplo, os *smartphones*, que acompanham o indivíduo em qualquer local, e os dispositivos inteligentes presentes nas residências, que conseguem captar qualquer informação dentro do ambiente que se encontram.

> Ultrapassamos, assim a necessidade de confinar aqueles que necessitam ser controlados. A flexibilidade e a ubiquidade da tecnologia da informação garantem a possibilidade de regulação dos processos sociais sem que seja necessário detê-los dentro de espaços institucionais físicos – contêineres territoriais (MENEZES NETO; MORAIS, 2018, p. 1151)

Outro aspecto presente na sociedade de controle é a formação das bolhas virtuais, composta por filtros *online* que identificam os gostos e as ações de um usuário e de outros que possuem gostos e ações semelhantes. São chamadas de bolhas dos filtros por Eli Pariser (2012, p. 11), que as conceitua como “mecanismos de previsão que criam e refinam constantemente uma teoria sobre quem somos e sobre o que vamos fazer ou desejar a seguir.” (PARISER, 2012, p. 11). José Wilson Correa Garcia (2020), expõe que,

> A bolha virtual é exatamente a “organização” de interações entre pessoas com base em seus próprios gostos e coisas que as identificam a partir de suas bases de dados. Cria-se, assim, uma interação onde a noção de que todo mundo pensa igual a todo mundo, passa a dominar a experiência do usuário na Internet, porque os algoritmos aproximam pessoas que têm uma base de dados parecida e distancia as que ele julga ser pessoas com base de dados diferente.

As bolhas virtuais funcionam mediante filtros personalizados, “primeiro, o filtro tenta entender quem é a pessoa e do que ela gosta. A seguir, oferece-lhe conteúdo e serviços adequados. Por fim, faz um ajuste fino para melhorar essa correspondência” (PARISER, 2012, p. 78). A bolha dos filtros “busca apresentar ao usuário uma lista de publicações que guarde relação com seu comportamento passado na rede, bem como por sugestões decorrentes de dados de comportamento de usuários com perfil similar” (GAMBA, 2021).

> Tal qual uma lente, a bolha dos filtros transforma inevitavelmente o mundo que vivenciamos, determinando o que vemos e o que não vemos. Ela interfere na inter-relação entre nossos processos mentais e o ambiente externo. Em certos casos, pode atuar como uma lente de aumento, sendo muito útil quando queremos expandir a nossa visão sobre uma área específica do conhecimento. No entanto, os filtros personalizados podem, ao mesmo tempo, limitar a variedade de coisas as quais somos expostos, afetando assim o modo como pensamos e aprendemos (PARISER, 2012, p. 58).

Tal mecanismo tem a capacidade de influenciar as decisões tomadas pelos usuários, uma vez que apresentam algumas possibilidades e bloqueiam outras, moldando a formação do indivíduo (PARISER, 2012, p. 78). Na bolha dos filtros é possível identificar todas as informações sobre determinado indivíduo, passando-se a ter conhecimento sobre suas preferências, assim, ao conhecer quais os tipos de incentivos que as pessoas respondem, aumenta-se o poder de manipulá-las (PARISER, 2012, p. 84).

> A manipulação de comportamento ocorre quando as análises preditivas são transformadas em ações por aqueles que detêm poder para tanto, sempre com a finalidade de modificar um comportamento, geralmente sem consciência daquele que está no polo passivo da relação de poder (MENEZES NETO; MORAIS, 2018, p. 1141).

Diante disso, na sociedade de controle, encontra-se a chamada modulação deleuziana, proposta por Gilles Deleuze (1992), no sentido de que “os controles são uma modulação, como uma moldagem auto-deformante que mudasse continuamente” (DELEUZE, 1992, p. 221). Nessa sociedade o controle atua por meio de mecanismos de poder que “intervêm na produção do desejo através de estímulos, evitando qualquer conotação coativa; eles visam a produção do desejo, e não sua mera repressão. [...] estimulando as motivações do indivíduo e induzindo seu querer” (RUIZ, 2004, p. 76).

A modulação deleuziana se apresenta de forma profunda e abrangente e subdivide-se em quatro conjuntos, quais sejam: jornalismo informativo, propaganda, manipulação midiática e modulação algorítmica (LEITÃO; SOARES, 2020, p. 164). A mais recente, e importante para esta pesquisa, é a modulação algorítmica, a qual corresponde a uma modulação executada por meio de algoritmos.

A modulação tem como objetivo “cristalizar nas consciências individuais, ideias, vontades, desejos, subjetividade” (LEITÃO;SOARES, 2020, p 166), enquanto os algoritmos são utilizados para encontrar padrões e construir perfis de modo a identificar os indivíduos de forma específica quanto aos seus gostos, desejos e preferências a fim de selecionar os conteúdos que se adequam àquele perfil, auxiliando, principalmente, o *marketing*. Neste sentido, Nicolas Samuel Gomes Leitão e Telmir de Souza Soares (2020, p.) afirmam que,

> A modulação necessita, nesse nosso tempo, da mediação de algoritmos que geram uma brilhante tática de sugestões, até mesmo de indução, nos consumidores alvos, alterando seu comportamento para fins de consumo baseado nos seus próprios rastros digitais de experiências anteriores.

Conforme expõe Castor M. M. Bartolomé Ruiz (2020, p. 75) “as sociedades contemporâneas investem pesadamente na construção de dispositivos e tecnologias que têm como objetivo central induzir ou produzir um tipo de desejo no indivíduo”. A

produção do desejo está relacionada com a presença dos algoritmos nas tecnologias da informação e com o controle operado por estas, o que provoca a modulação. Modular significa controlar (LEITÃO; SOARES, 2020, p. 164).

Assim, no cenário da sociedade de controle, conforme afirma Gilles Deleuze (1992), os indivíduos se tornaram divisíveis, “ser usuário dessas redes sociais é ser *dadificado*, reduzido a dados, a informação para futura modulações” (LEITÃO; SOARES, 2020, p. 166). A “dataficação” (MAYER-SCHONBERGER; CUKIER, 2013, p. 54) dos indivíduos que compõem a sociedade de controle é um dos pontos essenciais dessa pesquisa, pois a redução dos indivíduos a dados toca no ponto da proteção de dados pessoais, bem como contribui para a concretização da modulação. Sendo assim, o próximo Capítulo irá tratar sobre a evolução do regime jurídico referente a proteção de dados pessoais, presente no âmbito internacional e nacional.

2 EVOLUÇÃO DO REGIME JURÍDICO SOBRE A PROTEÇÃO DE DADOS PESSOAIS

Tendo em vista o uso de algoritmos pelas redes sociais para coleta de dados pessoais e, consequentemente, o tratamento desses, importante tratar sobre a legislação aplicada ao tema. Diante disso, esse Capítulo se propõe a apresentar a trajetória para a criação de leis sobre a proteção de dados pessoais, destacando a legislação no âmbito europeu e sua influência para a criação de uma legislação brasileira específica. Além disso, serão abordados alguns Projetos de Lei sobre o tema que foram apresentados entre os anos de 2019 e 2021.

2.1 DA LEGISLAÇÃO EUROPEIA

2.1.1 *General Data Protection Regulation*[2] (GDPR)

[2] Regulamento Geral de Proteção de Dados.

A Europa foi pioneira quando se fala em legislação sobre a proteção de dados pessoais. Em 1973 foi publicada uma resolução a qual “incentivava os países europeus a adotarem princípios mínimos na matéria” (DONEDA, 2020, p. 193), a fim de que mais tarde fosse realizada uma convenção que iria abordar o assunto de forma mais aprofundada.

> No contexto internacional, uma das consequências dessas inciativas precursoras foi a consciência de que um enfoque realizado exclusivamente a partir do direito interno não era suficientemente eficaz para o tema, dado que a coleta e tratamento de dados pessoais pode facilmente ser feito fora dos confins de um estado; daí que uma iniciativa de uniformização legislativa supranacional se mostrou necessária (DONEDA, 2020, p. 193).

Em 1981, o Conselho da Europa decidiu iniciar o processo para regulamentar a proteção de dados, por meio da Convenção 108 (UNIÃO EUROPEIA, 1981), a qual provocava “os estados-membros do Conselho da Europa e demais signatários da Convenção a adotar normas específicas para o tratamento de dados pessoais” (DONEDA, 2020, p. 194). Nesse sentido, segundo Danilo Doneda (2020, p. 195), “é possível considerar a Convenção 108 como ponto de referência inicial do modelo europeu de proteção de dados pessoais”.

A partir da construção dessa Convenção, outros países da Europa que já possuíam alguma legislação sobre o tema da proteção de dados começaram a adequar suas legislações, seguindo o padrão adotado pela Convenção, por outro lado, aqueles que ainda não haviam introduzido o tema no seu ordenamento jurídico, começaram a legislar sobre o assunto (DONEDA, 2020, p. 194).

Pensando em criar um modelo comum para a Europa, em 24 de outubro de 1995, foi aprovada a Diretiva 95/46/CE (UNIÃO EUROPEIA, 1995), a qual era um pouco mais específica, possuindo em sua redação “um amplo texto legal sobre a proteção de dados, que trazia princípios, direitos e deveres dos titulares de dados, além de outras diretivas gerais aos países membros para que adequassem suas legislações internas” (TEIXEIRA; ARMELIN, 2021, p. 21).

Desse modo, a Diretiva 95/46/CE efetivamente padronizou a proteção de dados pessoais no âmbito da União Europeia, referindo-se “à proteção das pessoas

singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados" (DONEDA, 2020, p. 195).

A Diretiva foi revogada pela entrada em vigor do *General Data Protection Regulation* (GDPR), promulgado em 2016 sob o Regulamento 2016/679 (UNIÃO EUROPEIA, 2016). Este tinha como finalidade "harmonizar as leis de privacidade de dados em todos os Estados membros da União Europeia" (TEIXEIRA; ARMELIN, 2021 p. 21). Assim, difere-se da Diretiva, uma vez que é aplicável a todos os países membros da União Europeia, ou seja, não é necessário que cada país adeque suas legislações internas como ocorreu anteriormente (DONEDA, 2020, p. 197). Nesse contexto, Tarcísio Teixeira e Ruth Maria Guerreiro da Fonseca Armelin (2021, p. 23) explicam que,

> A Diretiva, além de ter sido promulgada em uma época em que a transformação digital ainda era nascente, necessitava que cada país membro da União Europeia editasse normas internas para que as regras fossem aplicáveis. A diretiva tinha o caráter instrutório e dependia de harmonização interna dos países. Trazia princípios e direitos básicos de proteção aos dados pessoais dos cidadãos. De outra sorte, o regulamento atual, desde a sua eficácia plena, passou a ser diretamente aplicável a todos os Estados Membros da União Europeia, sem depender de qualquer tipo de normatização interna. Ainda, trouxe definições importantes que não continham na Diretiva auxiliando na sua imediata aplicabilidade, eliminando antigas disparidades e conflitos antes existente entre as legislações dos países membros (TEIXEIRA; ARMELIN, 2021, p. 23).

A criação de uma legislação única para o território europeu se deu em razão da necessidade de atualizar o regulamento sobre a proteção de dados pessoais, uma vez que o sistema de tratamento de dados pessoais desenvolveu-se com rapidez e se integrou ao mercado, transformando os dados em mercadorias (DONEDA, 2020, p. 191).

Assim, nota-se que o GDPR (UNIÃO EUROPEIA, 2016) unificou as normas sobre a proteção de dados pessoais na União Europeia, atualizando algumas normas da Diretiva 95/46/CE e evitando as divergências existentes entre as inúmeras legislações sobre o tema que vigoravam na Europa.

Além disso, o mais importante quanto ao advento do GDPR (UNIÃO EUROPEIA, 2016) foi a utilização de uma técnica legislativa, prevista em seus artigos 45 e 46, no

sentido de que para a transferência internacional de dados entre um Estado Membro da União Europeia e outro que não seja membro, é necessário que este também possua uma legislação referente a proteção de dados pessoais (DONEDA, 2020, p. 231).

> Artigo 45º. Transferência com base numa decisão de adequação. 1. Pode ser realizada uma transferência de dados pessoais para um país terceiro ou uma organização internacional se a Comissão tiver decidido que o país terceiro, um território ou um ou mais setores específicos desse país terceiro, ou a organização internacional em causa, assegura um nível de proteção adequado. Esta transferência não exige autorização específica (GDPR, 2016)
>
> Artigo 46º. Transferências sujeitas a garantias adequadas. 1. Não tendo sido tomada qualquer decisão nos termos do artigo 45º, 3, os responsáveis pelo tratamento ou subcontratantes só podem transferir dados pessoais para um país terceiro ou uma organização internacional se tiverem apresentado garantias adequadas, e na condição de os titulares dos dados gozarem de direitos oponíveis e de medidas jurídicas corretivas eficazes (GDPR, 2016).

Nesse sentido, “o regulamento europeu impôs diversas restrições para a transferência internacional de dados entre os países europeus e os demais países” (TEIXEIRA; ARMELIN, 2021, p. 28), sendo uma delas a necessidade de uma legislação específica sobre o tema no país que tenha interesse em realizar a transferência de dados.

Diante disso, “os Estados que não incorporassem em seus ordenamentos internos, normas de proteção de dados pessoais, poderiam sofrer penalidades, tais como barreiras econômicas e impossibilidade de transações financeiras” (SILVA, V. 2019, p. 58). Assim, para que o Brasil continuasse mantendo relações econômicas com os países da União Europeia foi necessário se enquadrar nas exigências previstas pela norma europeia, uma vez que os dispositivos legais existentes no ordenamento jurídico brasileiro não eram suficientes, pois não tratavam de modo específico sobre a proteção de dados pessoais.

Em face de tal problemática, será abordado a seguir sobre a legislação nacional referente a proteção de dados pessoais, desde os dispositivos constitucionais e infraconstitucionais que existem no ordenamento jurídico brasileiro até a Lei Geral de Proteção de Dados Pessoais (BRASIL, 2018), e, por fim, sobre alguns Projetos de Lei recentes.

2.2 DA LEGISLAÇÃO BRASILEIRA

2.2.1 Dispositivos constitucionais e infraconstitucionais

A proteção de dados no Brasil não é algo novo, apesar de poder ser considerada completa após a promulgação da Lei Geral de Proteção de Dados Pessoais – LGPD (BRASIL, 2018). Antes do advento da Lei (BRASIL, 2018) o ordenamento jurídico brasileiro tratava sobre a proteção de dados na Constituição Federal (BRASIL, 1988) e em legislações esparsas, quais sejam: Código Civil (BRASIL, 2002), Código do Consumidor (BRASIL, 1990), Lei de Cadastro Positivo (BRASIL, 2011) e o Marco Civil da Internet (BRASIL, 2014). Entretanto, cada lei regulamenta a proteção de dados pessoais conforme seu âmbito de incidência.

Na Constituição Federal (BRASIL, 2018) a proteção de dados pessoais começou a ser tratada no rol de direitos fundamentais do art. 5º, como proteção ao direito de personalidade, à liberdade de expressão (art. 5º, IX) e pelo direito à informação (art. 5º, XIV) (LUGATI; ALMEIDA, 2020, p. 10). Além disso, trata nos incisos X, XI e XII, respectivamente, sobre a inviolabilidade da intimidade e da vida privada, da casa e do sigilo dos dados, os quais também estão ligados a proteção de dados pessoais, pois tem relação com a proteção da intimidade e da privacidade da pessoa natural. Desse modo, observa-se que tais dispositivos conferem proteção a esfera privada da vida do indivíduo, na qual estão inseridos os dados pessoais.

Por sua vez, o Código Civil, Lei nº 10.406/2002 (BRASIL, 2002), prevê em seu artigo 21, a inviolabilidade da vida privada da pessoa natural, podendo esta requer ao Judiciário que faça cessar qualquer ato que viole sua vida privada. Em 2012, na V Jornada de Direito Civil foi aprovado o Enunciado 404, referente ao artigo 21 do Código Civil (BRASIL, 2002), contendo o seguinte texto,

> A tutela da privacidade da pessoa humana compreende os controles espacial, contextual e temporal dos próprios dados, sendo necessário seu expresso consentimento para tratamento de informações que versem especialmente o estado de saúde, a condição sexual, a origem racial ou étnica, as convicções religiosas, filosóficas e políticas (CONSELHO DA JUSTIÇA FEDERAL, 2012).

A Lei de Cadastro Positivo, nº 12.414/2011 (BRASIL, 2011), disciplina a “formação de banco de dados sob um conjunto de dados relativos às operações financeiras e de adimplemento para fins de concessão de crédito” (BIONI, 2021 p. 126). A Lei (BRASIL, 2011), “consolida a evolução do conceito de autodeterminação informativa no ordenamento, na medida em que coloca o consentimento como necessário para o compartilhamento de dados ser lícito” (MENDES apud LUGATI; ALMEIDA, 2020, p. 110). Todavia, com a LGPD (BRASIL, 2018), não mais é exigido o consentimento para a formação dos bancos de dados, uma vez que a Lei (BRASIL, 2018) prevê no inciso X do artigo 7º a proteção do crédito como base legal para o tratamento de dados pessoais.

Enquanto isso, o Código de Defesa do Consumidor, Lei nº 8.078/1990 (BRASIL, 1990), dispõe sobre os bancos de dados e cadastros de consumidores (BIONI, 2021, p. 125), em seu artigo 43 expressa que ao consumidor é assegurado o direito de acesso às informações existentes nos bancos de cadastros. Assim, prevê que “os cadastros e dados sejam objetivos, claros, verdadeiros e em linguagem de fácil compreensão” (art. 43, §1º).

Por outro lado, o Marco Civil da Internet, Lei nº 12.965/2014 (BRASIL, 2014), é o que mais se aproxima da LGPD (BRASIL, 2018), uma vez que trata sobre o direito a proteção da privacidade e dos dados pessoais no âmbito digital. No entanto, se limita as relações ocorridas na Internet, tendo como finalidade “assegurar os direitos e garantias do cidadão no ambiente eletrônico” (BIONI, 2021, p. 128). Assim, também garante ao indivíduo o direito ao não fornecimento a terceiros de seus dados pessoais, salvo mediante consentimento, que deve ser livre, expresso, informado e destacado (art. 7º, VII e IX).

Conforme tratam Lys Nunes Lugati e Juliana Evangelista de Almeida (2020, p. 12), o processo legislativo do Marco Civil da Internet (BRASIL, 2014) foi feito de modo apressado em razão do caso de espionagem revelado pelo ex-analista da Agência Nacional de Segurança dos Estados Unidos, Edward Snowden.

> Nesta lei, já há menção expressa ao consentimento e sua adjetivação, tendo em vista que, principalmente após o escândalo, buscou-se conferir proteção

> especial ao titular dos dados, dando a ele participação no processo de tratamento de dados (LUGATI; ALMEIDA, 2020, p. 12)

Nesse cenário de regulamentação expressa, mesmo que dispersa, da proteção de dados pessoais no Brasil, e considerando os interesses econômicos no âmbito internacional, o Brasil promulgou a Lei Geral de Proteção dos Dados Pessoais (LGPD), uma norma específica de proteção de dados pessoais, a qual entrou em vigor completamente no dia 1º de agosto de 2021 em razão da alteração feita pela Lei nº 14.010/2020, incluindo o inciso I-A ao artigo 65 da LGPD (BRASIL, 2018).

Essa alteração do momento da entrada em vigor da LGPD (BRASIL, 2018) se deu em razão da demora na criação da Agência Nacional de Proteção de Dados (ANPD), das dificuldades e custos envolvidos na implementação dos sistemas de segurança da informação e proteção de dados, e também, em razão da crise econômica e social causada pela pandemia do coronavírus (RAEFFRA; SANTOS, 2020).

Assim, os artigos 55-A a 55-L, 58-A e 58-B, os quais tratam sobre a ANPD, entraram em vigor em dezembro de 2018, os artigos 52, 53 e 54, referem as sanções administrativas, entraram em vigor em agosto de 2021, e os demais artigos, em setembro de 2020.

Sendo assim, antes de adentrar no tópico referente as bases legais da Lei Geral de Proteção de Dados Pessoais (BRASIL, 2018), importante tratar, de modo geral, sobre o Marco Civil da Internet (BRASIL, 2014), pois esse, ainda que não seja tão específico quanto a LGPD (BRASIL, 2018), aborda alguns pontos essenciais para o entendimento do regime jurídico aplicado ao tema dessa pesquisa.

2.2.2 Marco Civil da Internet (MCI)

O Marco Civil da Internet, foi introduzido no ordenamento jurídico brasileiro pela Lei nº 12.965/2014 (BRASIL, 2014), para regular o uso da Internet no Brasil, trazendo em seu texto o chamado tripé axiológico, previsto no artigo 3º, o qual se constitui pelos princípios da liberdade de expressão, da privacidade e da neutralidade da rede. Chiará

Spadaccini de Teffé e Maria Celina Bodin de Moraes (2017, p. 112) afirmam que, “enquanto a neutralidade da rede reforça a liberdade de expressão, a privacidade representa seu limite”.

> A liberdade de expressão, considerada como liberdade de externar ideias, juízos de valor e as mais variadas manifestações do pensamento, além de já ser amplamente protegida pelo constituinte, apresenta no MCI tutela destacada, sendo considerada um fundamento e um princípio para a disciplina do uso da internet no Brasil e condição para o pleno exercício do direito de acesso (TEFFÉ; MORAES, 2017, p.113).

No que diz respeito à privacidade, essa teve destaque em razão da circulação de informações pessoais na Internet (TEFFÉ; MORAES, 2017, p. 112). Assim, ante a ausência de uma lei que tratasse de modo específico sobre o tema da proteção de dados pessoais, mesmo que esses fossem considerados abrigados de maneira mais geral na forma de proteção de direitos da integridade moral presentes na Constituição Federal (BRASIL, 1988) e no Código Civil (BRASIL, 2002), o Marco Civil da Internet (BRASIL, 2014) fixou alguns direitos considerados essenciais para o usuário, tendo como base o controle e a autodeterminação informativa (TEFFÉ; MORAES, 2017, p. 124).

O Marco Civil da Internet (BRASIL, 2014) “trouxe para o ordenamento jurídico pátrio o princípio da neutralidade de rede e reforçou em seu texto o já consagrado constitucionalmente princípio da liberdade de expressão” (PONTIERI, 2018, p. 15), do mesmo modo, incluiu a proteção da privacidade, nesse caso, voltada para o âmbito da Internet.

> A lei assegura aos usuários o direito à proteção da privacidade e a informações claras e completas sobre a coleta, uso, armazenamento, tratamento e proteção de dados pessoais, e garante também que os dados pessoais não serão transferidos a terceiros, salvo expresso consentimento ou determinação legal (GARCIA, R., 2016).

O princípio da neutralidade da rede, foi tratado com mais destaque pelo Marco Civil da Internet (BRASIL, 2014), sendo previsto de forma detalhada no artigo 9º. Em relação a natureza jurídica da neutralidade da rede, Irineu Francisco Barreto Junior e Daniel César (2017, p. 71), sustentam que pode ser entendida sob três aspectos,

> Como um princípio que congrega outros princípios como transparência, liberdade de expressão e defesa da concorrência; como regra específica, determinando condutas a serem observadas, sendo possível a aplicação de sanções no caso de não observância; como arquitetura da Internet, determinando o funcionamento da rede e o acesso aos aplicativos online.

Por meio desse princípio deve-se “informar a construção de todo o arcabouço normativo da rede” (FORGIONI; MIURA, 2015, p. 1297). O princípio tem o objetivo principal de garantir um “tratamento isonômico ao tráfego de pacotes de dados na Internet”, não permitindo distinções sobre o conteúdo, cabendo ao usuário a decisão sobre como usar a Internet e quais dados acessar (SILVA, L., 2018, p. 28). Nesse sentido, “como princípio, a Neutralidade da Rede pode ser definida como determinação de que todas as comunicações devem ser tratadas de forma igual, qualquer que seja a informação, o destinatário ou a fonte” (BARRETO JUNIOR; CÉSAR, 2017, p. 69).

Irineu Francisco Barreto Junior e Daniel César (2017, p. 66), entendem que, em resumo,

> A Neutralidade da Rede determina que todas as conexões de dados devem ser tratadas de forma igual, qualquer que seja a informação, o destinatário ou a fonte. A Neutralidade da Rede relaciona-se as condutas aceitáveis e não aceitáveis por parte dos provedores de conexão, sendo esses proibidos de discriminar e bloquear aplicativos, degradar o tráfego na rede e agirem de forma transparente aos usuários com relação às medidas de gerenciamento da rede.

Entretanto, o Marco Civil da Internet (BRASIL, 2014) ao tratar sobre a neutralidade da rede (art. 9º), impôs que somente o responsável pela transmissão, comutação ou roteamento devem realizar o tratamento de forma isonômica, excluindo, assim, as plataformas de acesso aos conteúdos e aplicações (BARRETO JUNIOR; CÉSAR, 2017, p. 85). Assim, verifica-se que a regulamentação é específica, podendo existir tratamento não isonômico em outros casos, por exemplo, “discriminação na pesquisa a determinado conteúdo” (BARRETO JÚNIOR; CÉSAR, 2017, p. 85).

Importante destacar, por fim, seis possíveis riscos da ausência de neutralidade na rede, que são apresentados por João Victor Rozatti Longhi (2020, p. 116 - 117), sendo eles,

> 1. Filtragem pelos provedores de qual conteúdo é ou não acessado aos usuários; 2. Formação de monopólios verticais entre provedores de conteúdo, acesso e hospedagem com sensível diminuição do poder de escolha dos consumidores acerca do que acessam; 3. Controle de preços e formação de carteis; 4. Diminuição do tempo médio de velocidade para o consumidor final; 5. Restrição à inovação tecnológica; 6. Diminuição das possibilidades de expressão política na Internet.

Esses riscos trazem sérios impactos para os usuários da rede, na medida em que sem a neutralidade da rede os provedores de conteúdo poderão filtrar tudo que é ou não acessado, violando assim, a privacidade dos indivíduos, e, em razão da possibilidade de formação de monopólios entre os provedores de conteúdo, a liberdade de escolha dos consumidores será restringida.

Diante disso, observa-se que o tripé axiológico previsto pelo Marco Civil da Internet (BRASIL, 2014) estabeleceu normas para que o fornecimento e o uso da Internet ocorresse de forma isonômica, obedecendo a privacidade e a liberdade de expressão dos usuários. Ademais, ausente a neutralidade de rede evidente a produção de riscos aos usuários da Internet, havendo total descontrole dos conteúdos disponíveis, bem como a impossibilidade de se penalizar os provedores de internet que não observarem tal princípio. Portanto, é de extrema importância a presença da neutralidade de rede na Internet, assim como a garantia da privacidade e da liberdade de expressão.

Além disso, importante destacar que o Marco Civil da Internet (BRASIL, 2014) foi o primeiro dispositivo legal a tratar sobre o direito ao consentimento na Internet, uma vez que este já havia sido introduzido no ordenamento jurídico brasileiro na Lei do Cadastro Positivo (BRASIL, 2011), portanto, referia-se apenas ao consentimento para a proteção do crédito. Assim, no Marco Civil da Internet (BRASIL, 2014) o consentimento é um direito assegurado ao usuário no artigo 7º, VII e IX, o qual dispõe que somente é possível ao usuário fornecer seus dados pessoais a terceiros, registro de conexão e acesso a aplicações de Internet mediante o consentimento, devendo este ser livre, expresso e informado, bem como, nos casos de tratamento de dados pessoais, ocorrer de forma destacada das demais cláusulas contratuais.

Após tratar sobre o Marco Civil da Internet (BRASIL, 2014) importante observar as bases legais que atuam como suporte para a aplicação da Lei Geral de Proteção de Dados (BRASIL, 2018), essas estão previstas nos Capítulos I, II e III do artigo 1º ao

20, neles incluem-se, principalmente, fundamentos, princípios, requisitos para o tratamento de dados, sendo, portanto, direitos do titular.

2.2.3 Lei Geral de Proteção de Dados Pessoais (LGPD)

A Lei Geral de Proteção de Dados Pessoais (LGPD) inicia, em seu artigo 1º, tratando sobre o âmbito de incidência e seu objetivo. Assim, nota-se que a LGPD (BRASIL, 2018) versa sobre o tratamento de dados pessoais, seja em ambiente físico ou digital, feito por pessoa física ou jurídica de direito público ou privado e, tem como objetivo proteger os direitos fundamentais, nos quais se destacam o direito de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural. Ademais, dispõe o parágrafo único do mesmo dispositivo, que esta Lei se aplica a todo território nacional devendo ser observada por todos os entes federativos.

Tarcisio Teixeira e Ruth Maria Guerreiro da Fonseca Armelin (2021, p.30), expõem que,

> A proteção dos dados pessoais se insere na sociedade da informação como uma possibilidade de se tutelar o indivíduo diante dos potenciais riscos que o tratamento de dados poderia causar à sua personalidade, pois o que se visa proteger não são os dados em si, mas sim o seu titular, que poderá ser afetado em sua privacidade caso alguns limites não sejam estabelecidos.

Nesse sentido, apesar de a Lei ser chamada de Lei Geral de Proteção de Dados Pessoais (BRASIL, 2018) e dispor sobre o tratamento destes, seu foco principal é o indivíduo, titular dos dados. Isso porque tem como finalidade a proteção dos direitos fundamentais pertencentes a este, protegendo sua liberdade, privacidade e livre desenvolvimento da personalidade contra o tratamento inadequado dos dados pessoais. Portanto, importante destacar que a LGPD (BRASIL, 2018) não pretende interromper a coleta e o tratamento de dados pessoais, mas sim regulamentar esta prática para que ela ocorra de forma adequada, sem violar os direitos fundamentais.

O artigo 2º dispõe sobre os fundamentos da LGPD (BRASIL, 2018) que justificam o tratamento de dados pessoais. Para fins dessa pesquisa, destacam-se os incisos II, III e V, os quais tratam sobre a autodeterminação informativa, a liberdade de

expressão, de informação, de comunicação e de opinião e, do desenvolvimento econômico e tecnológico e a inovação.

Desse modo, “o direito a autodeterminação informativa proporciona ao indivíduo o controle sobre suas informações” (DONEDA, 2020, p. 161). Tarcisio Teixeira e Ruth Maria Guerreiro da Fonseca Armelin (2021, p. 33) declaram que esta,

> Consiste na capacidade do indivíduo em saber, com exatidão, quais de seus dados pessoais estão sendo coletados, com a consciência da finalidade para que se prestarão, para assim, diante de tais informações, tomar a decisão de fornecê-los ou não, levando-se em conta os benefícios/malefícios que o tratamento de seus dados poderão lhe acarretar. É o controle que o indivíduo possui sobre seus dados pessoais.

Os demais fundamentos, previstos no inciso III, o respeito a privacidade e a inviolabilidade da honra e da imagem, tem como base o disposto no texto constitucional, tendo em vista que tratam sobre direitos da personalidade. Assim, para que o titular dos dados pessoais seja protegido deve haver um equilíbrio entre o direito à liberdade de expressão e o direito à privacidade e a intimidade, também assegurados como fundamento para o tratamento de dados pessoais.

Tarcisio Teixeira e Ruth Maria Guerreiro da Fonseca Armelin (2021, p. 35), apontam que, “nos dias atuais não há que se falar em progresso sem a utilização de dados, os mesmos são a base de grandes conquistas tecnológicas e a tendência é de que cada vez mais o tratamento de dados seja a grande força motriz da econômica”. Assim, percebe-se que a proteção de dados pessoais somente é necessária, pois há desenvolvimento econômico e tecnológico e, a inovação, que se utiliza de dados pessoais para movimentar tanto a economia como a tecnologia.

Observa-se, a seguir, o disposto no art. 5º da LGPD (BRASIL, 2018), o qual apresenta os conceitos dos termos utilizados no texto legal, destacam-se, portanto: dado pessoal, dado pessoal sensível, banco de dados, titular, tratamento e consentimento.

> Art. 5º Para os fins desta Lei, considera-se:
> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de

> caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
> [...]
> IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;
> V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
> X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;
> XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

O dado pessoal corresponde a uma informação referente a pessoa natural que seja identificada ou identificável, ou seja, qualquer dado que possa identificar quem é aquele indivíduo, perpassando desde o nome até a geolocalização (TEIXEIRA; ARMELIN, 2021, p. 44), assim, são exemplos de dados pessoais, o nome, o CPF e a data de nascimento. Por outro lado, tem-se os dados pessoais sensíveis, os quais recebem “um tratamento diferenciado na lei [...], já que envolvem informações de foro íntimo” do indivíduo (TEIXEIRA; ARMELIN, 2021, p. 45).

Em relação aos dados pessoais sensíveis, estes possuem tal diferenciação legal, uma vez que possibilitam uma maior vulnerabilidade do indivíduo, sujeitando-o a diferenciação em razão de características da sua personalidade (BIONI, 2021, p. 83 – 84). No mesmo sentido, Danilo Doneda (2020, p. 144) entende que os dados pessoais sensíveis são “determinados tipos de informação que, caso sejam conhecidas e submetidas a tratamento, podem se prestar a uma potencial utilização discriminatória ou lesiva”. Tendo em vista esse caráter especial dos dados sensíveis estes apresentam maiores riscos aos titulares do que outras informações que não são consideradas dados sensíveis.

Diante disso, o art. 5º, inciso II da LGPD (BRASIL, 2018), contém um rol específico de quais são os dados pessoais considerados sensíveis. Assim, são dados pessoais sensíveis, aqueles que são possíveis identificar a origem racial ou étnica, a convicção religiosa, a opinião política, a filiação a sindicato ou a organização de caráter religioso, filosófico ou político, os dados referentes à saúde ou à vida sexual, e por fim, os dados genéticos e biométricos, que sejam vinculados a uma pessoa natural.

Em seguida, tem-se o banco de dados, que nada mais é do que um conjunto de dados pessoais, os quais podem ser “tanto físico ou eletrônico” (TEIXEIRA; ARMELIN, 2021, p. 45). Danilo Doneda (2020, p. 142) afirma que “os bancos de dados consistem, basicamente, em conjuntos de informações organizadas segundo uma determinada lógica”. Ou seja, é o local onde os dados coletados são armazenados de modo organizado até o momento de serem tratados e deles seja extraída a informação.

> Um banco de dados deve ser necessariamente atrelado à ideia de um sistema de informação, cuja dinâmica explicita, sequencialmente, um processo que se inicia pela coleta e estruturação dos dados, perpassa a extração de uma informação que, por fim, agrega conhecimento (BIONI, 2021, p. 33).

O titular dos dados é aquele quem detém os dados que serão coletados para o tratamento. A titularidade possui extrema importância, pois apenas há proteção dos dados pessoais de pessoas vivas (TEXEIRA; ARMELIN, 2021, p. 46). Já o tratamento, refere-se a qualquer operação feita com os dados, sendo necessário para a extração de informações dos dados coletados (TEIXEIRA; ARMELIN, 2021, p. 46). Segundo afirma Marcos César Botelho (2020, p. 195), o tratamento de dados é fundamental para a seleção de informações úteis, que irão atribuir valor à atividade econômica que for desenvolvida.

Por fim, tem-se o consentimento, o qual representa a manifestação do titular sobre concordar ou não com o tratamento de seus dados devendo este ser livre, informado e inequívoco (art. 5º, XII). Segundo Danilo Doneda (2020, p. 293) “o consentimento compreende um poder conferido à pessoa de modificar sua própria esfera jurídica, com base na expressão de sua vontade”. Desse modo, “o titular deve ter pleno conhecimento de quais dados estão sendo captados e exatamente para qual fim ele será utilizado, o qual perfaz a inequivocabilidade do consentimento” (TEIXEIRA; ARMELIN, 2021, p. 46).

> O consentimento do titular para o tratamento de seus dados pessoais é um dos pontos mais sensíveis de toda a disciplina de proteção de dados pessoais; por meio dele, o direito civil tem a oportunidade de estruturar, a partir da consideração da autonomia da vontade, da circulação de dados e dos direitos fundamentais, uma disciplina que ajuste os efeitos desse consentimento à natureza dos interesses em questão (DONEDA, 2020, p. 292).

Em seguida, no artigo 6º, estão previstos os princípios, que devem ser observados para o tratamento dos dados pessoais, além da boa-fé “diretriz principiológica de fundo ético e espectro eficacial jurídico” (GAGLIANO; PAMPLONA FILHO, 2017, p. 128). O princípio da boa-fé, no âmbito da LGPD (BRASIL, 2018) reflete o dever de cooperação, o qual deve ser cumprido na relação entre os agentes de tratamento e os titulares de dados pessoais (NOGUEIRA; ESTÊVES, 2020). Além disso, o conteúdo dos princípios previstos na LGPD (BRASIL, 2018) demonstra a,

> repercussão das funções da boa-fé objetiva, na proporção em que há alusões a propósitos legítimos, devidamente esclarecidos, proporcionais e não excessivos, que garanta a consulta e o acesso gratuito e facilitado; bem como a prevenção da ocorrência de dados (NOGUEIRA; ESTÊVES, 2020).

Apesar dos demais princípios previstos no referido dispositivo legal e a necessidade do diálogo entre eles na resolução de casos concretos, esta pesquisa se limita a tratar sobre o princípio da transparência, previsto no inciso VI do artigo 6º da LGPD (BRASIL, 2018), pois esse está diretamente ligado a base legal do consentimento, o qual é solicitado a todo indivíduo que deseje se cadastrar em alguma rede social.

A transparência, já tratada no CDC (BRASIL, 1990) de forma mais geral (art. 6º, III; 43 e 46) como dever lateral geral decorrente do princípio da boa-fé objetiva, no contexto da LGPD (BRASIL, 2018), refere-se à necessidade de garantir ao titular dos dados informações sobre o tratamento de seus dados pessoais. Bruno Ricardo Bioni (2021, p. 188) afirma que “a prestação de uma informação só tem razão de ser se ela ocasionar transparência no fluxo dos dados pessoais”. Nesse sentido, as informações prestadas ao titular dos dados devem ser disponibilizadas de forma clara, precisa e de fácil acesso. Sob esta perspectiva, Tarcisio Teixeira e Ruth Maria Guerreiro da Fonseca Armelin (2021, p. 53) declaram que,

> A transparência pressupõe que o titular terá livre acesso às informações claras e precisas sobre o tratamento de seus dados pessoais, o que não significa, entretanto, um acesso irrestrito, já que ele não poderá ter acesso ao segredo industrial de um negócio ou a outras informações essenciais à realização do negócio.

Observa-se, portanto, que o objetivo do princípio da transparência, em relação a proteção de dados pessoais, é o de conferir ao titular dos dados, o acesso as

informações referentes ao tratamento de seus dados pessoais, ou seja, quais dados são coletados, como são armazenados, qual a finalidade dessa coleta, existência ou não de compartilhamento com terceiros, e entre outros, exceto nos casos em que os dados estão sob sigilo ou estejam relacionados ao segredo comercial ou industrial.

Nesse sentido, ao titular é conferido o direito ao acesso facilitado às informações sobre o tratamento de seus dados, conforme dispõe o artigo 9º da LGPD (BRASIL, 2018). Além disso, o mesmo artigo prevê que as informações deverão ser disponibilizadas de forma clara, adequada e ostensiva. Nesse contexto, estão consolidados os princípios do livre acesso e da transparência, os quais, segundo Tarcisio Teixeira e Ruth Armelin (2021, p. 66),

> Garantem ao titular de dados o acesso facilitado a todas as informações sobre o tratamento dos seus dados, possibilitando que o titular tenha a certeza de que seus dados serão coletados, com quem o controlador poderá compartilhá-los, quais serão as responsabilidades dos agentes e quais são os seus direitos como titular.

A respeito dos requisitos para o tratamento dos dados pessoais, o artigo 7º apresenta as hipóteses legais que conferem validade ao tratamento dos dados pessoais. Por outro lado, em relação aos dados pessoais sensíveis, em razão do seu caráter mais vulnerável, as hipóteses para o seu tratamento estão previstas no artigo 11 da LGPD (BRASIL, 2018). Quando se fala em coleta de dados feita pelas plataformas digitais o mais comum é a requisição do consentimento do titular, previsto no início I dos artigos 7º e 11, pois é por meio deste que o titular manifesta sua vontade, concordando ou não com a coleta de seus dados pessoais para o tratamento.

Vale ressaltar que, apesar de o consentimento estar previsto no primeiro inciso do artigo 7º, não há hierarquia quanto as hipóteses legais do dispositivo legal. Isso porque cada um atende a uma situação específica, sem depender da incidência de outro para que seja aplicável. No entanto, de acordo com Tarcisio Teixeira e Ruth Armelin (2021, p. 56),

> Pode-se afirmar que o consentimento do titular mesmo diante de novas possibilidade legais de tratamento, continua a ter certa preferência sobre os demais, pois geralmente facilita a obrigação do agente de tratamento em demonstrar que o tratamento foi feito dentro de uma hipótese legal, ante o princípio da *accountability* (prestação de contas).

Já no que se refere aos dados pessoais sensíveis, o artigo 11 apresenta no inciso primeiro hipótese na qual o titular dos dados deve consentir. Nesse caso, além do consentimento ser livre, inequívoco e informado, deverá ser feito de forma específica, destaca e para finalidades específicas, ou seja, não pode ser um consentimento genérico/geral. E, no inciso segundo, hipóteses em que pode haver tratamento de dados pessoais sensíveis, sem a necessidade do consentimento do titular, por exemplo, o exercício regular de direitos, em contrato e em processo judicial, administrativo e arbitral, hipótese prevista na alínea “d”.

Ademais, “o pedido de consentimento deve ser dado de uma forma inteligível e de fácil acesso, com o propósito de processamento de dados anexado a esse consentimento” (TEIXEIRA; ARMELIN, 2021, p. 56), ao passo que “o consentimento deve ser claro e distinguível de outros assuntos e ser fornecido de uma forma inteligível e de fácil acesso, usando linguagem clara e objetiva” (TEIXEIRA; ARMELIN, 2021, p. 56 – 57). Isso porque, conforme trata Danilo Doneda (2020, p. 296),

> O consentimento para o tratamento de dados pessoais toca diretamente em uma série de elementos da própria personalidade, ainda que não no sentido exato da disposição desses elementos. Ele assume com mais propriedade as vestes de um ato do titular cujo efeito será de autorizar um determinado tratamento para os dados pessoais.

Na sequência, o artigo 8º da LGPD (BRASIL, 2018) trata sobre o modo pelo qual o consentimento deve ser fornecido, “por escrito ou por outro meio que demonstre a manifestação de vontade do titular”, inclusive, deverá estar em cláusulas destacadas das demais no contrato, caso o consentimento seja concedido por escrito, e referir-se a finalidades determinadas, ou seja, ao consentimento deve estar vinculado a um propósito, especificando para que serão utilizados os dados fornecidos.

Nesse sentido, em atenção ao princípio da transparência a previsão legal é no sentido de que “para cada finalidade será colhido um consentimento específico, sendo que o titular consente a utilização de seus dados pessoais para um propósito informado previamente” (TEIXEIRA; ARMELIN, 2021, p. 62).

O consentimento, conforme disposto no artigo 5º, inciso XII da LGPD (BRASIL, 2018), deve ser livre, informado e inequívoco. No que diz respeito a ser informado, esse “deve ser ostensivo e a sua percepção é indispensável” (TEIXEIRA; ARMELIN, 2021, p. 62), ou seja, é necessário que o titular tenha fácil acesso à informação, bem como que seja evidente que foi informado corretamente.

Em relação ao adjetivo livre, Bruno Ricardo Bioni (2021, p. 183) reconhece que “é muito provável que haja um diálogo com o Código Civil brasileiro para se interpretar toda a adjetivação do consentimento à luz dos defeitos do negócio jurídico”. Tal afirmação se torna clara quando a LGPD (BRASIL, 2018) veda o tratamento de dados pessoais quando houver vício de consentimento (art. 8º, §4º). Nesse sentido, um consentimento livre representa a manifestação da vontade do titular dos dados feita sem qualquer vício do consentimento, como erro, coação e lesão.

O adjetivo inequívoco, por fim, caracteriza o consentimento de modo que “não paire dúvidas de que o titular consentiu a utilização de seus dados pessoais para aquele fim” (TEIXEIRA; ARMELIN, 2021, p. 62). Isto é, a manifestação da vontade do titular deve se dar de forma objetiva, demonstrando o consentimento. Ademais, o consentimento, em determinadas situações, deverá ser específico, como é o caso dos dados sensíveis (art. 11, I) e do tratamento de dados de crianças e adolescentes (art. 14, §1º).

O consentimento fundamenta-se na autodeterminação dos titulares de dados pessoais, pois essa é utilizada para caracterizar a natureza jurídica e os efeitos do consentimento (DONEDA, 2020, p. 296). O consentimento, ao ser requerido para o tratamento de dados pessoais, se relaciona com elementos da personalidade do titular, assumindo os atos deste “cujo efeito será de autorizar um determinado tratamento para os dados pessoais” (DONEDA, 2020, p. 296).

Danilo Doneda (2020, p. 296) analisando os efeitos do consentimento, expõe que deve ser feita uma ponderação da autodeterminação, concluindo que existem duas possibilidades de analisá-lo, como instrumento para a autodeterminação e como instrumento de legitimação para que os dados pessoais sejam utilizados por terceiros. O consentimento ao mesmo tempo que confere ao titular de dados a manifestação de

sua escolha, garante aos que coletam os dados legitimidade para coletar, armazenar e compartilhar.

O artigo 17 da LGPD (BRASIL, 2018) trata sobre os direitos do titular, dispondo que toda pessoa natural tem assegurada a titularidade de seus dados pessoais, no sentido de que os dados pessoais pertencem apenas a uma pessoa natural determinada, bem como a estas são garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade. Nesse sentido, Tarcisio Teixeira e Ruth Armelin (2021, p. 89) afirmam que,

> Por mais evidente que possa parecer o transcrito nesse artigo o seu conteúdo é de vital importância, pois revela ao indivíduo sobre a titularidade de seus dados pessoais, que integram sua personalidade, que deverão estar sob o "manto" da liberdade, privacidade e intimidade.

Assim, percebe-se que a proteção e garantia do direito fundamental de liberdade, além de ser objetivo da Lei Geral de Proteção de Dados Pessoais (BRASIL, 2018), é também direito assegurado ao titular dos dados pessoais, o que demonstra a preocupação do legislador em preservar os direitos fundamentais relacionados ao indivíduo e aos riscos do tratamento de dados pessoais.

No âmbito da legislação brasileira uma decisão é automatizada quando não há interferência humana, quando afeta os interesses do titular de dados pessoais e quando se destina a definir o perfil do titular dos dados pessoais (LIMA; SÁ, 2020, p. 234). Segundo o disposto no artigo 20 da LGPD (BRASIL, 2018), uma decisão automatizada é aquela que afeta os interesses do titular dos dados pessoais, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

No que diz respeito as decisões automatizadas, conforme Tarcísio Teixeira e Ruth Maria Guerreiro da Fonseca Armelin (2021, p. 96) esse artigo foi incluído na LGPD (BRASIL, 2018) com o intuito de manifestar a "preocupação com o limite de influência da decisão de uma máquina sobre a vida das pessoas, considerando-se que muitas vezes a análise de dados se dará de forma automatizada". Conforme o dispositivo objetiva-se,

> Assegurar ao titular de dados que o mesmo poderá pedir a revisão de decisão tomada única e exclusivamente de forma automatizada e que possam afetar seus interesses, seja para definir seu perfil pessoal, profissional, de consumo, de crédito e até mesmo perfis de sua personalidade (TEIXEIRA; ARMELIN, 2021, p. 94).

Tal disposição é chamada de direito à explicação, sendo “uma consequência do princípio da transparência” (LIMA; SÁ, 2020, p. 232), uma vez que, após uma decisão automatizada que causa prejuízo ao titular dos dados, este pode requerer a revisão da tomada dessa decisão.

> Nem sempre o resultado colhido por um algoritmo refletirá a realidade do titular de dados, podendo o mesmo sofrer prejuízos caso não lhe seja possibilitada a revisão da decisão. Em decisões que levaram à tomada da decisão. Não é porque foi um robô que tomou a decisão que o direito à transparência e ao livre acesso será tolhido do usuário, respeitados, evidentemente, os segredos comerciais e industrial (TEIXEIRA; ARMELIN, 2021, p. 95).

A proposta inicial previa que esta revisão seria feita por pessoa natural. Todavia, o texto incluído na LGPD (BRASIL, 2018) comporta divergências (LIMA; SÁ, 2020, p. 232), ao excluir a figura da pessoa natural da redação do dispositivo “a revisão poderá ser feita tanto por uma pessoa natural como novamente por uma máquina” (TEIXERA; ARMELIN, 2021, p. 95).

Importante destacar, ainda, que a LGPD (BRASIL, 2018) não reproduziu a lei europeia na íntegra. Quando se fala em *profiling*, elaboração de um perfil a partir do processamento dos dados (LIMA, 2019, p. 35 – 36), o GDPR (UNIÃO EUROPEIA, 2016), tratou de conceituar o termo em seu artigo 4º, da seguinte forma,

> Profiling significa qualquer forma de tratamento automatizado de dados pessoais que consista na utilização de dados pessoais para avaliar determinados aspectos pessoais relativos a uma pessoa natural, em particular para analisar ou prever aspectos relativos ao desempenho profissional, situação econômica, saúde, preferências pessoais, interesses, confiabilidade, comportamento, localização ou movimentos (UNIÃO EUROPEIA, 2016).

Além disso, em seu artigo 22, o GDPR (UNIÃO EUROPEIA, 2016) expõe que o titular dos dados não deve ser submetido à uma decisão que seja exclusivamente automática, como é o caso do *profiling*. Por sua vez, a LGPD (BRASIL, 2018) não

tratou de conceituar o termo em seu artigo 5º, bem como não apresenta uma vedação específica a tal prática, dispondo apenas que, caso ocorra a “perfilização” (ZANATTA, 2019), o titular dos dados terá o direito à explicação (art. 20).

Nesse contexto, segundo Rafael Zanatta (2019, p. 7), a Lei Geral de Proteção de Dados Pessoais (BRASIL, 2018) “é *menos restritiva* com relação à perfilização do ponto de vista da (i) ausência de um conceito jurídico expresso e (ii) ausência de uma norma geral proibitiva ao *profiling*, como ocorre na União Europeia”.

Desse modo, percebe-se que a Lei Geral de Proteção de Dados Pessoais (BRASIL, 2018) apresenta normas a serem seguidas para que o tratamento de dados seja feito de forma adequada e legal, bem como tem por finalidade proteger os direitos fundamentais do titular dos dados pessoais.

Em relação as plataformas digitais, a LGPD (BRASIL, 2018) dispõe normas para que os dados sejam coletados adequadamente, como é o caso da requisição do consentimento do titular, no entanto, para que este seja válido, as plataformas digitais devem observar o princípio da transparência, previsto na LGPD(BRASIL, 2018). Além disso, no que diz respeito as decisões automatizadas, o titular dos dados têm direito à explicação caso seja afetado por uma decisão tomada unicamente com base em tratamento automatizado de dados pessoais, e quanto ao *profiling* a LGPD (BRASIL, 2018) se mostra silente em relação a sua conceituação e a sua previsão legal.

2.2.4 Projetos de Lei

Após a promulgação da Lei Geral de Proteção de Dados Pessoais (BRASIL, 2018), alguns projetos de lei foram apresentados entre os anos de 2019 e 2021 e estão tramitando no Congresso Nacional. Tais projetos tratam sobre assuntos relacionados com a transparência, com os algoritmos e com a Inteligência Artificial.

Em setembro de 2019 foi apresentado o Projeto de Lei nº 5.051 (BRASIL, 2019), de autoria do Senador Styvenson Valentim, a fim de regulamentar o uso da Inteligência

Artificial no Brasil por meio da fixação de princípios. No artigo 3º dispõe que “a disciplina do uso da Inteligência Artificial no Brasil tem por objetivo a promoção e a harmonização da valorização do trabalho humano e do desenvolvimento econômico” (BRASIL, 2019). Tal proposta justifica-se com base na adoção de sistemas de Inteligência Artificial presentes no mercado, constituindo uma tecnologia que gera ganhos de produtividade e melhorias na qualidade. Ao apresentar a justifica do referido projeto o Senador destaca que,

> “nos termos da proposição, todo sistema de Inteligência Artificial terá a supervisão de uma pessoa humana, de forma compatível com cada aplicação. Com isso, é possível aliar as vantagens trazidas por essa inovação tecnológica com a necessária segurança, evitando que eventuais equívocos do sistema automatizado provoquem consequências indesejadas” (BRASIL, 2019).

Em fevereiro de 2020, foi apresentado o Projeto de Lei nº 21 (BRASIL, 2020a), de autoria do Deputado Federal Eduardo Bismarck, o qual propõe-se a estabelecer princípios, direitos e deveres para o uso da Inteligência Artificial no Brasil, ficando conhecido como marco legal da Inteligência Artificial. Além disso, tem como objetivo determinar as diretrizes para a atuação dos entes federativos, das pessoas físicas e jurídicas, de direito público ou privados e dos entes sem personalidade jurídica. Em setembro de 2021 foi apresentada a redação final e remetido ao Senado Federal, onde se encontra atualmente.

> O PL 21/2020 lista aspectos que dependerão de regulamentação e coloca nas mãoes de órgãos e entidades setoriais a prerrogativa para isso, como agências reguladoras e o Banco Central. Eles também deverão monitorar o risco de sistemas de IA. O governo, porém, não poderá regular o tema, exceto quando for “absolutamente necessário” (SANTA ROSA, 2021).

Giovanni Santa Rosa (2021) expõe que especialistas criticaram a tramitação do Projeto de Lei nº 21/2020, alegando que as discussões foram apressadas, sem consulta pública, deixando prevalecer o interesse das *big techs*. Além disso, expõe que o referido Projeto apresenta alguns aspectos polêmicos, pois prevê que “qualquer regulamentação do assunto só deve estabelecer punições a quem desenvolve ou administra esses sistemas se houver culpa ou dolo” (SANTA ROSA, 2021).

Em julho de 2020, foi apresentado o Projeto de Lei nº 2630 (BRASIL, 2020b), de autoria do Senador Alessandro Vieira, o qual pretende instituir a Lei Brasileira de

Liberdade, Responsabilidade e Transparência na Internet, estabelecendo normas, diretrizes e mecanismos de transparência para provedores de redes sociais e de serviços de mensageria privada, a fim de garantir segurança e ampla liberdade de expressão, comunicação e manifestação do pensamento, sendo mais conhecimento como “PL das Fake News”. Em resumo, o referido projeto (BRASIL, 2020b) tem como finalidade criar medidas de combate à disseminação de conteúdo falso nas redes sociais. Além disso, prevê a aplicação de sanções aos provedores de redes sociais e de serviços de mensageria privada.

Edgard Monteiro (2020) ao fazer uma relação do PL 2630/2020 com a liberdade de expressão e informação, afirma que,

> É anti-nacional a existência de mecanismos capazes de subverter a compreensão de um cidadão sobre a própria realidade, a partir do momento em que ele se torna usuário e consumidor de produtos e de mercadorias anunciados por perfis cujas identidades são incertas. [...] Em uma rede social, onde as notícias são selecionadas e colocadas em destaque de acordo com o patrocínio e, portanto, com o poder econômico de quem as divulga, é dado a todo usuário o poder real de escolha entre opções e alternativas concretas de produtos (notícias políticas)? As redes sociais se tornaram determinantes no cenário eleitoral de todos os países, de tal maneira que se torna necessário o controle popular dessas plataformas para que nos coloquemos autênticos e soberanos em nossa política.

Em agosto de 2020 foi apresentado o Projeto de Lei nº 4120 (BRASIL, 2020c), de autoria do Deputado Federal Bosco Costa, o qual tem o objetivo de disciplinar o uso de algoritmos na internet, de modo a assegurar transparência no uso das ferramentas computacionais que posam induzir a tomada de decisão ou atuar sobre as preferências dos usuários. Desse modo, observa-se que o referido Projeto (BRASIL, 2020c) é o que mais se aproxima do assunto tratado nesta pesquisa, uma vez que dispõe sobre o uso de algoritmos nas redes sociais e a garantia da transparência.

O Projeto nº 4120 (BRASIL, 2020c) fundamenta-se na publicidade direcionada, utilizada pelos provedores para promover a divulgação de bens e serviços na Internet, tendo como preocupação o fato de que os algoritmos utilizados nesses sistemas são geralmente protegidos pelo segredo industrial, o que impede aos usuários terem acesso as regras que governam a operação, e, além disso, a questão de que os algoritmos são tão complexos que, mesmo que os usuários tivessem acesso as informações, seu funcionamento seria dificilmente compreendido pelo cidadão

comum. Em razão disso, importante destacar alguns artigos do referido Projeto de Lei (BRASIL, 2020c).

Primeiramente, o artigo 2º trata sobre expressões utilizadas pela legislação. Nesse contexto, destacam-se dois sistemas de decisão, quais sejam: o sistema de decisão automatizada, previsto no inciso I, o qual consiste em um processo computacional que facilita a tomada de decisões humanas ou toma decisões em nome de pessoas de forma automatizada, e, o sistema de decisão automatizada de elevado risco, previsto no inciso II, o qual consiste em um sistema de decisão automatizada que apresenta risco ao disponibilizar informações imprecisas, injustas, tendenciosas ou discriminatórias que podem afetar decisões humanas ou um sistema que toma decisões, ou facilita a tomada dessas com base em avaliações sistemáticas e extensas do comportamento de pessoas, analisando e prevendo aspectos sensíveis da vida do usuário.

Em seu artigo 4º, impõe aos provedores de sistema de decisão automatizada o dever de produzir anualmente relatório de impacto, publicar este relatório na internet, na forma de extrato, informar aos usuários, de forma destacada e recorrente que faz uso de sistema de decisão automatizada de elevado risco e, elaborar e publicar na internet guia de orientação para os usuários, contendo informações sobre o uso dos sistemas e sobre os riscos.

Conforme artigo 7º, caberá ao Poder Público a elaboração e publicação na internet de guia contendo padrões e boas práticas para o desenvolvimento e a operação de sistemas de decisão automatizada de elevado risco.

Por fim, o artigo 9º informa que a inobservância das normas previstas, sujeita o provedor de aplicações à sanções, conforme o caso, que poderão ser aplicadas de forma isolada ou cumulativa, são elas: advertência, multa de até 10% do faturamento do grupo econômico no Brasil no seu último exercício, suspensão temporária das atividades ou proibição de exercício das atividades.

Em dezembro de 2020 o Projeto de Lei nº 4120 (BRASIL, 2020c) foi apensado ao Projeto de Lei nº 21 (BRASIL, 2020a). Entretanto, em setembro de 2021 o Projeto

(BRASIL, 2020c) foi desapensado em face da declaração de prejudicialidade em razão da aprovação de Subemenda Substitutiva Global ao Projeto de Lei nº 21 (BRASIL, 2020a). Diante disso, atualmente o referido Projeto de Lei encontra-se arquivado.

Por último, no mês de março de 2021 foi apresentado o Projeto de Lei nº 872, de autoria do Senador Veneziano Vital do Rêgo, o qual dispõe sobre os marcos éticos e as diretrizes que fundamentam o desenvolvimento e o uso da Inteligência Artificial no Brasil. O Projeto foi proposto sob a justifica de que a Inteligência Artificial tem um potencial de aumentar a produtividade em até 40% e de otimização do tempo, assim, diante de um cenário em que diversos países já implementaram técnicas voltadas para o desenvolvimento da Inteligência Artificial e devido sua importância para o desenvolvimento econômico e social do país, importante que se tenha legislações que tratem sobre o tema.

Em fevereiro de 2022, a presidência do Senado Federal determinou a tramitação conjunta do Projeto de Lei nº 21/202, com os Projetos de Lei nº 5.051/2019 e 872/2021, por entender que estes tratam de tema correlato.

Ante o exposto, verifica-se que, apesar de promulgada lei específica sobre a proteção de dados pessoais, LGPD (BRASIL, 2018), há temáticas relacionadas com o ambiente virtual que ainda não foram contempladas pela legislação brasileira. Neste sentido, tramitam atualmente no Congresso Nacional, projetos de lei que têm como objetivo incluir no ordenamento jurídico normas que regulamentem as questões referentes a *fake news*, o uso de algoritmos nas plataformas digitais e a aplicação da Inteligência Artificial.

Após feitas as considerações sobre o regime jurídico que trata do tema, ou seja, as leis vigentes e projetadas aplicáveis à proteção de dados pessoais e sobre os projetos de lei recentes apresentados ao Congresso Nacional, passa-se a tratar sobre a utilização de algoritmos pelas redes sociais para o tratamento de dados pessoais e suas consequências.

3 A UTILIZAÇÃO DE ALGORITMOS PELAS REDES SOCIAIS

Segundo Manuel Castells (2011, p. 566) o termo “rede” corresponde a um conjunto de nós que estão interconectados, a qual constitui estruturas que conseguem se expandir, ilimitadamente, e, integrar novos nós desde que possuam os mesmos códigos de comunicação. Nesse sentido, conforme mencionado no Capítulo 1, as redes sociais são “um conjunto de participantes autônomos, unindo ideias e recursos em torno de valores e interesses compartilhados” (MARTELETO, 2001, p. 72).

Em razão do crescimento das tecnologias e o aumento do fluxo de informações na Internet os indivíduos começaram a integrar mais os espaços digitais. Por esse motivo, ante a enorme quantidade de informações presentes no ambiente virtual, inseriu-se os algoritmos, códigos capazes de obter as informações de cada usuário e fazer previsões sobre o comportamento a partir delas.

Desse modo, “o uso crescente dos algoritmos acompanha a intensa digitalização da nossa comunicação, dos nossos arquivos e das nossas expressões simbólicas. Também expressa a grande automação das nossas atividades produtivas” (SILVEIRA, 2019, p. 17). As redes sociais, conforme afirma Sérgio Amadeu da Silveira (2019, p. 20),

> São organizadas por algoritmos que definem o que devemos ver e quantos dos nossos amigos ou seguidores devem visualizar um conteúdo que publicamos, entre outras ações. O resultado desses filtros seriam bolhas que reúnem e interligam aqueles que têm o mesmo padrão e as mesmas características.

De acordo com o que foi tratado nos Capítulos anteriores, para que os algoritmos possam realizar previsões é necessária a coleta de dados e o tratamento destes, pois só assim é possível extrair uma informação relevante. Diante de uma coleta desmoderada de dados na Internet foi fundamental a criação de leis que garantissem a proteção de dados pessoais. Assim, promulgou-se, em 2018, no Brasil, a Lei Geral de Proteção de Dados Pessoais (BRASIL, 2018), que prevê hipóteses legais para que o tratamento de dados seja feito de forma correta e sem violar os direitos fundamentais, como a privacidade e a liberdade.

Uma das hipóteses legais que confere validade ao tratamento de dados, prevista na LGPD (BRASIL, 2018) diz respeito ao consentimento (art. 7º, I; 11, I), conforme exposto no Capítulo 2. Segundo Bruno Ricardo Bioni (2021, p. 132), o consentimento representa “uma carga principiológica que procura conformar, justamente, a ideia de que o titular dos dados pessoais deve ser empoderado com o *controle* de suas informações pessoais e, sobretudo, na sua autonomia da vontade”.

Diante desse cenário, esta pesquisa busca identificar se há violação ao princípio da transparência, bem como se há modulação deleuziana na sociedade brasileira, significando que esta tenha a estrutura de uma sociedade de controle, o que, nas palavras de Deleuze (1992) é onde os indivíduos se tornam dados, os quais são utilizados pelos algoritmos para realizar a modulação, ou seja um controle que se opera com base nos interesses individuais. Para tanto, nos próximos tópicos será tratado, respectivamente, sobre a hipótese legal do consentimento, se essa é válida ou não, e, sobre a técnica de *profiling* e suas consequências.

3.1 A POSSÍVEL VIOLAÇÃO AO PRINCÍPIO DA TRANSPARÊNCIA PREVISTO NA LGPD

A possibilidade de violação do princípio da transparência, previsto no art. 6º, IV da LGPD (BRASIL, 2018) começa a tomar forma quando, para que ocorra a coleta e o tratamento de dados de forma válida no âmbito das redes sociais, os indivíduos precisam manifestar que concordam em fornecer seus dados pessoais. Nesse sentido, surgiram os termos de uso e as políticas de privacidade, os quais trazem textos longos, com letras pequenas, escondidos por trás de dizeres como, “selecione o item se leu e concorda”. Segundo Bruno Ricardo Bioni (2021, p. 166), “por meio de tal técnica contratual, colher-se-ia o prescrito e necessário consentimento para legitimar toda e qualquer operação de tratamento de dados pessoais”.

É a partir da segunda geração de normas de proteção de dados pessoais que se inicia o protagonismo do indivíduo sobre a proteção de seus dados pessoais (BIONI, 2021, p. 133).

> A segunda geração de leis transfere para o próprio titular dos dados a responsabilidade de protegê-los. Se antes o fluxo das informações deveria ser autorizado pelo Estado, agora cabe ao próprio cidadão tal ingerência que, por meio do consentimento, estabelece as suas escolhas no tocante à coleta, uso e compartilhamento dos seus dados pessoais (BIONI, 2021, p. 115).

No Brasil, a segunda geração é representada pela Lei do Cadastro Positivo (BRASIL, 2011) promulgada no Brasil em 2011, a qual previa em seu artigo 4º até 2019 a necessidade do consentimento para a abertura de cadastro. A partir de 2019 deixou-se de ser necessário, pois a LGPD (BRASIL, 2018) prevê como hipótese legal o tratamento de dados pessoais quando destinados à proteção do crédito (art. 7º, X).

Já na terceira geração das leis inicia-se a introdução da ideia da autodeterminação informativa. No Brasil, essa geração corresponde ao Marco Civil da Internet (BRASIL, 2014), o qual assegura no artigo 7º o direito do usuário a não ter seus dados fornecidos a terceiros sem o seu consentimento, bem como o direito ao consentimento livre, expresso, informado e destacado sobre o tratamento de seus dados pessoais.

Bruno Ricardo Bioni (2021, p. 115) afirma que, “neste estágio, as normas de proteção de dados pessoais procuraram assegurar a participação do indivíduo sobre todos os movimentos dos seus dados pessoais”. Em razão disso, o indivíduo, ao participar das etapas do tratamento dos seus dados pessoais, detém mais controle sobre seus dados e informações (BIONI, 2021, p. 115). Todavia, a autodeterminação informativa somente se concretiza na quarta geração de leis sobre a proteção de dados pessoais, que no Brasil é retratada na Lei Geral de Proteção de Dados Pessoais (BRASIL, 2018).

> A proteção de dados é vista, por tais leis, como um processo mais complexo, que envolve a participação do indivíduo na sociedade e leva em consideração o contexto no qual lhe é solicitado que revele seus dados, estabelecendo meios de proteção para as ocasiões em que a sua liberdade de decidir livremente é cerceada por eventuais condicionantes (DONEDA, 2015, p. 373).

Assim, a autodeterminação informativa diz respeito a capacidade do próprio cidadão ter controle sobre seus dados pessoais e informações (DONEDA, 2020, p. 161), sendo possível que este possa escolher quando conceder seus dados pessoais e quais deles irá conceder. Assim, para que as informações pessoais fossem protegidas, utiliza-se

o consentimento como uma das técnicas legislativa para legitimar as etapas do tratamento de dados pessoais (BIONI, 2021, p. 133 – 134). Estabeleceu-se, portanto, que o consentimento estaria ligado ao elemento volitivo, ou seja, com a autonomia privada do titular dos dados pessoais (BIONI, 2021, p. 134).

> O consentimento do titular para o tratamento de seus dados pessoais é um dos pontos mais sensíveis de toda a disciplina de proteção de dados pessoais; por meio dele, o direito civil tem a oportunidade de estruturar, a partir da consideração da autonomia da vontade, da circulação de dados e dos direitos fundamentais, uma disciplina que ajuste os efeitos desse consentimento à natureza dos interesses em questão (DONEDA, 2020, p. 292).

O consentimento, também tratado no Marco Civil da Internet (BRASIL, 2014), recebia os adjetivos livre, expresso, informado e destacado, para que fosse considerado válido. No âmbito da LGPD (BRASIL, 2018) não é diferente, o consentimento é uma das hipóteses legais pela qual poderá ser realizado o tratamento de dados pessoais (art. 7º, I). Desse modo, para que a Lei (BRASIL, 2018) atinja seu objetivo de proteger os direitos fundamentais o consentimento deve ser livre, informado e inequívoco (art. 5º, XII) e referir-se a finalidades determinadas (art. 8º, §4º) e, no caso de dados pessoais sensíveis, o consentimento também deve ser feito de forma específica, destacada e para finalidades específicas (art. 11, I).

Em resumo, livre significa que o consentimento não pode ser concedido sob algum vício do consentimento, o indivíduo deve escolher de forma livre sem intromissão de algo ou alguém na sua conduta. Informado indica que o indivíduo deve receber todas as informações sobre o que será feito com seus dados pessoais, para então decidir se irá consentir ou não. Por fim, inequívoco representa que não pode haver dúvidas de que o usuário consentiu ou não de forma voluntária. Sob esta perspectiva, conforme expõem Gustavo Tepedino e Chiara Spadaccini de Teffé (2020, p. 93),

> O consentimento representa instrumento de manifestação individual no campo dos direitos da personalidade e tem o papel de legitimar que terceiros utilizem, em alguma medida, os dados de seu titular. Ele compreende a liberdade de escolha, sendo meio para a construção e delimitação da esfera privada. Associa-se, portanto, à autodeterminação existencial e informacional do ser humano, mostrando-se imprescindível à proteção do indivíduo e à circulação de informações.

Danilo Doneda (2020, p. 292) propõe que o consentimento, ao representar a autonomia privada em determinados momentos, seja interpretado como instrumento de manifestação da escolha individual e seja objeto de referência direta dos valores fundamentais, como à privacidade e à imagem. Nesse contexto, o autor expõe que “o consentimento compreende um poder conferido à pessoa de modificar sua própria esfera jurídica, com base na expressão de sua vontade” (DONEDA, 2020, p. 293).

O possível problema referente ao consentimento reside no fato de que os usuários das redes sociais não são informados adequadamente, pois lhe são apresentados um item para selecionar e concordar com os termos de uso e a “facultatividade” de ler estes, uma vez que o usuário não é obrigado a ler para prosseguir com sua atividade *online* basta marcar que leu e concorda com os termos, mesmo sem os ter lido, o que configura um contrato de adesão. Ademais, o usuário que deseja participar da plataforma não pode ser contra a coleta e o compartilhamento de seus dados, somente lhe sendo apresentada a opção de que concorda com o tratamento de seus dados, caso não concorde este não consegue prosseguir com o cadastro.

Nesse contexto, Sérgio Amadeu da Silveira (2021, p. 36) afirma que “o efeito desse consentimento é pequeno, pois as pessoas, na maioria das vezes, não têm opção de negar a entrega de determinados dados diante da necessidade de uso do serviço”. No mesmo sentido, Danilo Doneda (2020, p. 293) afirma que,

> O confronto com situações reais revela que, em tais situações, a alternativa a não revelação dos dados pessoais pelo seu titular costuma ser uma – por vezes, brutal – renúncia a determinados bens ou serviços. A disparidade de meios e de poder entre a pessoa de quem é demandado o consentimento para utilização dos dados pessoais em contemplação da realização de um contrato e aquele que os pede faz com que a verdadeira opção que lhe reste seja, tantas vezes, a de “tudo ou nada”, “pegar ou largar”.

Bruno Ricardo Bioni (2021, p. 145 – 156) apresenta alguns estudos empíricos que tratam de investigar o comportamento dos usuários diante de situações em que há coleta de seus dados pessoais, como por exemplo, para a publicidade direcionada. Na quarta pesquisa apresentada pelo autor, a qual foi realizada na Universidade de Bochum (Alemanha) em 2019, foram analisados os avisos de *cookies*, se havia transparência em relação as práticas de tratamento de dados pessoais nas plataformas, e a constante evasão do consentimento.

O estudo apontou uma falha, pois não trazia informações de forma adequada, bem como não provocava uma interação dos usuários com a tecnologia empregada. Ademais, realizou-se um teste considerando a linguagem dos avisos de notificação, neste os usuários se manifestaram no sentido de que a linguagem utilizada é técnica e que, mesmo lendo as informações, ainda não conseguem entender perfeitamente o que está sendo transmitido.

Percebe-se, assim, que os usuários, na maioria das vezes, não leem os termos e, quando leem, não conseguem entender perfeitamente as informações. Isso prejudica a existência de um consentimento válido, o que Bruno Ricardo Bioni (2021, p. 166), ao tratar sobre as políticas de privacidade, chama de consentimento falho, dizendo que,

> tal mecanismo tem se mostrado falho por inúmeras razões, seja porque ele reforça a aventada assimetria do mercado informacional, seja porque se trata de uma ferramenta que não capacita, efetivamente, o cidadão para exercer controle sobre as suas informações pessoais (BIONI, p. 166).

Ademais, afirma Bruno Ricardo Bioni (2021, p. 161) que, há uma falsa escolha do usuário quando este é submetido apenas a manifestá-la escolhendo pela opção de concordar, no sentido de que “a lógica do mercado e da sociedade da informação arquitetam essa (falsa) escolha, já que, para fazer parte do jogo, deve-se aceitar o convite mediante o ‘concordo’ em compartilhar os ‘meus’ dados pessoais”. No mesmo sentido, Danilo Doneda (2020, p. 195) entende tal cenário chamando-o de mito do consentimento.

> O problema derivado de uma transposição rasa do consentimento negocial para o consentimento ao tratamento de dados pessoais está presente em toda a crítica ao “mito do consentimento”. Tais problemas são, basicamente, reflexos da adaptação de uma estrutura formal e pretensamente neutra a uma realidade que apresenta apenas uma falsa semelhança com o ambiente no qual o consentimento é um real instrumento de realização da autonomia privada e pode compreender uma escolha ideológica (DONEDA, 2020, p. 195).

Em conjunto com o consentimento encontra-se o princípio da transparência, uma vez que para o indivíduo manifestar um consentimento válido este deve ser informado adequadamente. Para tanto, tem-se a necessidade de uma transparência no

momento de transmitir as informações aos usuários, deixando claro quais dados são coletados e para qual finalidade eles serão utilizados, pois “apenas com uma informação adequada o cidadão estará capacitado para controlar seus dados” (BIONI, 2021, p. 184).

Conforme sustenta Eli Pariser (2012, p. 156), a transparência, além de estar relacionada a revelação do interior de um sistema, “também significa que os usuários compreendem intuitivamente o funcionamento do sistema”, ou seja, não basta a apresentação de como o sistema funciona, os indivíduos devem ser capazes de entender as informações que estão sendo transmitidas.

O princípio da transparência estabelece que deve haver clareza na concessão das informações, estas devem ser disponibilizadas de forma clara, adequada e ostensiva (art. 9º da LGPD), bem como devem ser claras, precisas e de fácil acesso (art. 6º, VI da LGPD). Tais adjetivos representam um aspecto qualitativo da informação, atestando que esta deve ser perceptível pelo indivíduo, bem como que este possa entendê-las sem maiores esforços. Além disso, deve ser prestada em uma quantidade suficiente, para que haja celeridade no entendimento da mensagem, pois “o excesso de informação também desinforma” (BIONI, 2021, p. 185). Desse modo, o autor afirma que,

> A quantidade de informações pode prejudicar a sua qualidade, ainda que tais critérios não se confundam. O critério qualitativo liga-se à ideia de uma informação original e imprevisível que equaliza a disparidade informacional entre consumidor e fornecedor. Ao passo que a quantidade de informações é o seu plano consequente, verificando-se se tais informações originais e imprevisíveis são *suficientes* para despertar no consumidor uma compreensão adequada (BIONI, 2021, p. 186).

A partir da observação da rede social Instagram (META, 2010) e análise de suas políticas referentes a coleta de dados pessoais, percebe-se que estas não são apresentadas ao usuário de modo ostensivo, pois localizam-se nas configurações do aplicativo, ou seja, no ato de cadastrar suas informações pessoais o usuário tem que marcar a opção de que concorda com os termos de uso da rede social, lendo os termos apenas se tiver interesse. Além disso, ao fazer a leitura das políticas de dados da referida rede social, estas informam que foram atualizadas em janeiro de 2022, porém os usuários não foram informados sobre esta atualização, bem como não foram

direcionados ao local onde pode ser feita a leitura dos novos termos e, não foi oportunizado nova opção para concordar com os termos atualizados.

Outro exemplo é a rede social TikTok (BYTEDANCE, 2016), a qual também oferece uma opção de concordar e a leitura facultativa de sua política de privacidade aos usuários que queiram se cadastrar na plataforma. Um aspecto importante é que essa rede social disponibiliza seu uso mesmo para quem não seja cadastro. Entretanto, informa em sua política de privacidade que, as informações serão coletadas mesmo que o usuário não crie uma conta, mas interaja com a plataforma. A rede social expõe, ainda, que irá notificar o usuário sobre eventuais alterações materiais em sua política de privacidade.

Já a rede social Twitter (TWITTER INC., 2006) disponibiliza além da política de privacidade os termos de uso de cookies. No entanto, sua política de privacidade, apesar de ser diferente das outras, pois apresenta uma estrutura dinâmica, identificando cada tópico com uma cor específica e um resumo das principais informações que o usuário precisa ter conhecimento, também se mostra bastante extensa e como uma “concordância automática” de que quando o usuário faz o cadastro da plataforma ele está concordando com todos os termos.

Importante mencionar que as empresas tendem a se manifestar sobre a falta de transparência em razão da necessidade de preservar o sigilo do negócio. Ocorre que, a transparência diz respeito a informar o usuário sobre o motivo para ter seu dado pessoal coletado e o que será feito com ele. Assim, conferir maior transparência de seus atos de modo a modificar a forma de apresentação das políticas de privacidade, como por exemplo, além de utilizar um texto mais objetivo, também colocar a opção de concordar ou não em cada cláusula referente ao tratamento de dados pessoais, não irá prejudicar o sigilo do negócio, pois não é necessário que tais informações secretas estejam no termo de política de privacidade.

O referido exemplo se mostra apropriado, pois, como já mencionado no Capítulo 2, o consentimento deve se referir a finalidades adequadas, portanto, para cada situação que corresponda ao tratamento de dados pessoais, como a coleta, o armazenamento, o compartilhamento, deve haver um consentimento específico.

Ante o exposto, verifica-se que no ambiente das redes sociais os usuários precisam manifestar seu consentimento sem o devido acesso a informações claras, precisas, adequadas e ostensivas, fazendo com que o consentimento não apresente a vontade real do indivíduo. Desse modo, visualiza-se um embate entre a previsão legal da Lei Geral de Proteção de Dados Pessoais (BRASIL, 2018) que busca proteger o titular dos dados pessoais, colocando como necessária a transparência para se obter um consentimento verídico, e a realidade, em que o usuário tem sua liberdade de escolha limitada em razão da falta de transparência na transmissão das informações sobre a coleta e o tratamento dos dados pessoais e na falta de escolha de não poder optar pela não concordância com os termos da plataforma.

3.2 A POSSÍVEL EXISTÊNCIA DA MODULAÇÃO ALGORÍTMICA NA SOCIEDADE BRASILEIRA

A possibilidade de existência de uma modulação algorítmica na sociedade brasileira se dá pelo fato de esta se inserir em um contexto no qual estão presentes características da sociedade da informação e da sociedade de controle, em especial os algoritmos e a vigilância ubíqua.

Tendo em vista o tratado no Capítulo 1, entende-se que a sociedade da informação é aquela constituída pelas tecnologias da informação e comunicação, e se desenvolve a partir das informações e dos dados (SIQUEIRA JUNIOR, 2007, p. 2). Já a sociedade de controle é aquela marcada pela presença constante de mecanismos de tecnologia da informação que exercem uma vigilância ininterrupta no cotidiano dos indivíduos, bem como identifica-os como dados e tem como objetivo encontrar a motivação dos indivíduos (RUIZ, 2004, p. 90).

Os algoritmos estão incluídos de tal forma no dia a dia dos indivíduos que estes não percebem a atividade desempenhada por esses códigos, ou seja, a memorização dos hábitos e o direcionamento de conteúdos (SOUZA, 2019, p. 579 – 580). Fato é que, os algoritmos foram implementados para aprender e influenciar o comportamento dos

usuários, por isso fazem uma filtragem das informações presentes na Internet, a fim de identificar e selecionar aquelas que mais se encaixam no perfil do usuário (ROSSETTI; ANGELUCI, 2021, p. 11).

Nesse sentido, os algoritmos tiveram grande importância ao auxiliar a ciência mercadológica, na medida em que foi observado serem ineficientes as propagandas distribuídas sem nenhum propósito, já que eram desperdiçadas com um público que não tinha o intuito de consumir o que estava sendo anunciado (BIONI, 2021, p.15). Eli Pariser (2012, p. 10), afirma que, “a fórmula dos gigantes da internet para essa estratégia de negócios é simples: quanto mais personalizadas forem suas ofertas de informações, mais anúncios eles conseguirão vender” e, a partir disso, aumentam-se as chances de os indivíduos comprarem os produtos ofertados.

Ocorre que, além de um controle realizado pela publicidade por customização e direcionamento para os destinatários mais propensos ao consumo de determinados produtos ou serviços, atualmente, identifica-se um controle do impulso e do desejo humano. Isso porque, verifica-se no cenário atual uma distopia em que a Inteligência Artificial é capaz não só de identificar padrões de comportamento humano na Internet, mas também antecipar e direcionar somente aqueles conteúdos que sejam compatíveis com os desejos do usuário.

Visualiza-se, portanto, o papel dos algoritmos, os quais atuam com a finalidade de contribuir com a publicidade direcionada, fazendo com que os indivíduos realmente consumam os produtos e serviços, uma vez que cada usuário recebe publicidade somente daquilo que tem interesse (BIONI, 2021, p. 15). Além disso, os algoritmos exercem um papel fundamental na identificação das preferências dos usuários e na formação de seu perfil, colocando-o em uma bolha dos filtros (PARISER, 2012).

> A coleta de dados dos usuários pelas empresas na rede constrói um terreno propício para o trabalho dos algoritmos que realizam a filtragem de conteúdo, os quais, a partir da análise e correlação de dados, são capazes de traçar um perfil único de cada usuário, levando em consideração suas inclinações, preferências e aquilo que busca encontrar quando acessa a *internet* (BASTOS; VON ENDE, 2020, p. 20).

Para tanto, é utilizada “uma técnica estatística aplicada que consiste num mecanismo automatizado de processamento de grandes volumes de dados cuja função central é a extração de padrões que gerem conhecimento” (BRUNO, 2008, p. 13) chamada de *data mining* ou mineração de dados. Essa técnica consiste em “identificar e precisar o perfil do potencial consumidor, seus hábitos e outras informações necessárias à tomada de decisões táticas e estratégicas” (BIONI, 2021, p. 34). No mesmo sentido,

> Consiste na busca de correlações, recorrências, formas, tendências e padrões significativos a partir de quantidades muito grandes de dados, com o auxílio de instrumentos estatísticos e matemáticos. Assim, a partir de uma grande quantidade de informação em estado bruto e não classificada, torna-se possível identificar informações de potencial interesse (DONEDA, 2020, p. 150).

A partir dessa técnica tem-se o chamado *profiling* “em que os dados pessoais de um indivíduo formam um perfil a seu respeito para a tomada de inúmeras decisões” (BIONI, 2021, p. 88). Segundo Danilo Doneda (2020, p. 148 – 149), este mecanismo consiste na “elaboração de perfis de comportamento de uma pessoa a partir de informações que ela disponibiliza ou que são colhidas. [...] pode ser aplicada a indivíduos, bem como estendida a grupos”.

Para Sérgio Amadeu da Silveira (2021, p. 39) “um dos principais modos de controle que os gestores das plataformas possuem sobre seus usuários se dá pela modulação das opções e dos caminhos de interação e de acesso aos conteúdos publicados”. Joyce Souza, Rodolfo Avelino e Sérgio Amadeu da Silveira (2021, p. 10) sustentam que, para ser realizada a modulação é fundamental conhecer aquele que será modulado, portanto “é necessário reduzir o campo de visão dos indivíduos ou segmentos que serão modulados” (SILVEIRA, 2021, p. 40).

> O processo de modulação começa por identificar e conhecer precisamente o agente modulável. O segundo passo é a formação do seu perfil e o terceiro é construir dispositivos e processos de acompanhamento cotidiano constantes, se possível, pervasivos. O quarto passo é atuar sobre o agente para conduzir o seu comportamento ou opinião (SILVEIRA, 2021, p. 41).

Ao identificar o perfil dos consumidores formam-se agrupamentos de usuários que possuem os mesmos interesses, a chamada bolha dos filtros (PARISER, 2012). Por sua vez, Bruno Henrique Miniuchi Pelizzari e Irineu Francisco Barreto Junior (2019, p. 58) chamam tal cenário de “confinamento”, como consequência da presença dos

algoritmos, que ao serem alimentados por dados dos usuários, conseguem selecionar quais possuem as mesmas preferências e juntá-los em grupos (PELIZZARI; BARRETO JUNIOR, 2019, p. 58).

A partir da formação dos perfis e das bolhas dos filtros há um grande volume de dados, *Big Data*, os quais passam por análises tendo como objetivo, “descobrir padrões e conexões que de outra forma seriam invisíveis e que podem fornecer informações valiosas sobre os usuários que os geraram (SILVEIRA, 2019, p. 22). Segundo Sérgio Amadeu da Silveira (2019, p.22) é por meio do conhecimento obtido por essas análises que empresas conseguem ganhar vantagem frente as demais empresas e escolher qual a melhor decisão para seu negócio .

Desse modo, Sérgio Amadeu da Silveira (2019, p. 63) afirma que o tratamento de dados pessoais por meio das tecnologias de *Big Data* tem como objetivo final “modular o comportamento das pessoas, levando-as a encontrar mais certas mensagens do que outras”. Isso porque, com o tratamento dos dados pessoais, obtêm-se informações as quais possibilitam o direcionamento dos conteúdos na Internet, sendo um instrumento fundamental para realizar a modulação dos indivíduos, ou seja, moldá-los conforme o teor dos conteúdos, uma vez que os usuários deixarão de receber todos os tipos de conteúdo, passando a receber apenas aqueles que tenham relação com suas preferências.

A modulação consiste na perda da autonomia do usuário, pois este, em relação a escolha de comprar ou não um produto ainda tem poder de escolha. No entanto, no que diz respeito ao acesso dos conteúdos, o indivíduo somente terá acesso aqueles relacionados com seus interesses que foram identificados pela Inteligência Artificial, por exemplo quando se pesquisa sobre determinado produto, o usuário tem total liberdade de escolher qual irá comprar e se irá comprar, porém, nunca mais deixará de receber informações associadas a esse conteúdo. O mesmo ocorre com as informações pesquisas pelo usuário, as quais também são utilizadas para construir a bolha virtual, e direcionar somente informações que sejam compatíveis, semelhantes as pesquisas anteriormente.

Nesse contexto, a bolha dos filtros funciona como uma lente, transformando o mundo que conhecemos e determinando aquilo que pode ou não ser visto, de modo que interfere na relação entre nossa mente e o ambiente que vivemos (PARISER, 2012, p. 58). Nesse sentido, Eli Pariser (2012, p. 58) complementa dizendo que os filtros personalizados funcionam como limitadores das informações que o usuário recebe, bem como afetam a forma de pensar e aprender.

Os usuários têm a impressão de que estão escolhendo os conteúdos que desejam visualizar, produtos que desejam comprar, quando na verdade estão sendo objeto de modulação, ou seja, controle dos seus interesses. Trata-se, portanto, de uma ilusão de liberdade de escolha provocada nas pessoas pelos mecanismos de *big data* (TAVARES, 2019). Eli Pariser (2012, p. 78) declara que, "ao apresentar algumas possibilidades e bloquear outras, a bolha dos filtros influencia nossas decisões. E, assim, molda a pessoa na qual nos transformamos".

> O tratamento de "*big data*" literalmente, grandes bases de dados por meio de técnicas computacionais cada vez mais desenvolvidas pode levar a análises probabilísticas e resultados que, ao mesmo tempo que atingem os interesses de uma parcela específica da população, retiram a capacidade de autonomia do indivíduo e o seu direito de acesso ao consumo de bens e serviços e a determinadas políticas públicas, por exemplo (MULHOLLAND, 2018, p. 173).

Assim, percebe-se a atuação da modulação algorítmica nas redes sociais, em que os usuários estão cada vez mais envolvidos por dispositivos conectados à Internet, e, consequentemente, à atividade dos algoritmos, ou seja, a vigilância ubíqua. Os usuários são submetidos a regulação algorítmica, que trata da "fixação de padrões de conduta e ao monitoramento e a coleta de dados " (SILVEIRA, 2020, p. 65). Nesse sentido, "os sistemas algorítmicos podem alterar nossa liberdade de escolha ao restringirem as opções que nos são apresentadas nas redes sociais" (SILVEIRA, 2019, p. 61).

> Pensar em liberdade é pensar em possibilidade de escolha dentre várias escolhas que podemos fazer. Porém, se as opções são limitadas não temos livre-arbítrio em sua totalidade: independente da escolha – dentre qualquer uma oferecida – ela será pré-determinada (TAVARES, 2019, p. 142 – 143).

Bruna Bastos e Luiza Berger von Ende (2020), ao tratarem sobre a possibilidade de haver violações aos direitos fundamentais da igualdade, da liberdade de expressão e

de escolha, da dignidade da pessoa humana e a da não-discriminação no direcionamento de anúncios na Internet feito por algoritmos, sustentam que a realidade em que os indivíduos estão inseridos, ou seja, uma sociedade de controle, voltada para a coleta e o tratamento de dados pessoais,

> Tem o poder de impactar de forma direta na liberdade de escolha do usuário, especialmente no tocante ao direcionamento de anúncios feitos em decorrência dessa lógica dos algoritmos, da filtragem e da criação de um perfil para cada pessoa, na medida em que o usuário só terá acesso àquilo que os algoritmos pré-determinam que ele possa visualizar (BASTOS; VON ENDE, 2020, p. 22).

Eli Pariser (2012, p. 15) afirma que “por definição, um mundo construído a partir do que é familiar é um mundo no qual não temos nada a aprender”. Em razão disso, o autor declara que “se a personalização for excessiva, poderá nos impedir de entrar em contato com experiências e ideias estonteantes, destruidoras de preconceitos, que mudam o modo como pensamos sobre o mundo e sobre nós mesmos” (PARISER, 2012, p. 15).

A onipresença do ambiente virtual contribui para a ampliação e permanência do controle na sociedade, de modo que não é mais necessário um espaço físico para que o controle seja exercido. Na sociedade atual os aparelhos digitais conectados à Internet acompanham o indivíduo, por isso a supervisão não ocorre mais com a restrição da liberdade, mas sim com a exposição exercida de forma livre pelos próprios indivíduos (HAN, 2017). Nesse sentido, em um local em que os indivíduos são mantidos em bolhas com filtros invisíveis, expondo suas informações sem perceber, há uma ilusão de liberdade, já que não é possível enxergar os “muros” que os cercam.

Diante disso, identifica-se uma modulação algorítmica presente na sociedade brasileira, uma vez que os cidadãos estão inseridos em uma sociedade de controle, na qual opera-se uma vigilância ubíqua e, por meio do uso de algoritmos nas redes sociais, efetua-se uma modulação no comportamento dos usuários, ao pré-determinar e direcionar os conteúdos, tanto publicidade quanto informações, que estes receberão ao utilizarem a Internet, ou seja, os indivíduos são colocados em uma bolha, recebendo somente conteúdos que tenham relação com seus interesses.

Nesse sentido, “a personalização pode nos levar a uma espécie de determinismo informativo, no qual aquilo que clicamos no passado determina o que veremos a seguir” (PARISER, 2012, p. 16). Assim, os indivíduos não têm autonomia sobre suas decisões futuras, pois aquilo que irão visualizar será resultado da previsão dos algoritmos e não de sua própria decisão.

CONCLUSÃO

O presente trabalho de conclusão de curso buscou na medida e dimensão de um trabalho acadêmico de graduação identificar se a utilização de algoritmos pelas redes sociais ocasionaria alguma forma de violação do princípio da transparência, previsto no art. 6º, IV da LGPD (BRASIL, 2018) e, consequentemente, se cabe a denúncia da existência da modulação deleuziana na sociedade brasileira.

O estudo tomou como base o referencial teórico de pesquisa bibliográfica que se apoiou não somente, mas com destaque nos autores, Manuel Castells, Jeremy Bentham, Michel Foucault, Gilles Deleuze, Sérgio Amadeu da Silveira, Tarleton Gillespie, Christian Fuchs, Byung-Chul Han, Eli Pariser, Yuval Noah Harari, Danilo Doneda, Bruno Ricardo Bioni, Tarcisio Teixeira e Ruth Armelin. O resultado da pesquisa permitiu reconhecer características importantes da sociedade contemporânea que foram detalhadas no tratamento dos conceitos fundamentais da sociedade da informação e da sociedade de controle.

Além de trabalhar com os conceitos fundamentais como categorias que permitiram compreender a pertinência do tema principal relativo ao uso da modulação por meio de algoritmos e efetiva quebra do princípio da transparência, o presente trabalho tratou de fazer um levantamento do regime jurídico aplicável a questão fundamental proposta, dividindo-se a pesquisa e uma introdução que traz a legislação europeia, para efeito de reconhecimento da extraterritorialidade do problema, e, de forma mais detalhada e criteriosa dos principais documentos legislativos brasileiros. Nesse sentido, de *lege lata* e *lege ferenda* cuidou-se de reconhecer na lei vigente e mesmo projetada os mais importantes dispositivos legais que tratam da proteção de dados

pessoais sobretudo no ambiente digital para posteriormente trabalhar o tema central a luz dos acertos e erros da lei brasileira.

O primeiro capítulo tratou da sociedade da informação e da sociedade de controle e seus respectivos elementos constitutivos. Em cada uma cuidou-se de explicar como surgiu e como é possível identificá-las. Desse modo, concluiu-se que a sociedade da informação consiste em uma sociedade a qual se desenvolve a partir de informações e dados, tendo como elementos principais a Internet, as redes sociais, os algoritmos e o *Big Data*. Por sua vez, a sociedade de controle é a sociedade marcada pela existência do controle que se opera pelas tecnologias da informação, o qual está associado ao poder e a motivação dos indivíduos e, tem como elementos principais a vigilância ubíqua, a bolha dos filtros e a modulação deleuziana.

No segundo capítulo tratou-se da evolução do regime jurídico aplicado a proteção de dados, subdividindo-se este capítulo em legislação europeia e legislação brasileira. No âmbito europeu demonstrou-se que a Europa foi pioneira na criação de uma legislação específica sobre o tema. Cuidou-se, assim, de explicar sobre a Convenção 108, sobre a Diretiva 45/96/CE e, por fim, sobre o Regulamento 2016/679 e a promulgação do Regulamento Geral de Proteção de Dados (GDPR), sendo este o mais específico e influenciador dos demais países a legislarem sobre o tema também de forma específica, e, inclusive a lei original que inspirou o regime jurídico brasileiro que trata do tema.

No que diz respeito ao âmbito nacional, cuidou-se de apresentar inicialmente os dispositivos legais que tratavam sobre a proteção de dados antes do advento da Lei Geral de Proteção de Dados Pessoais (BRASIL, 2018), observou-se que estes se dividem em dispositivos constitucionais e infraconstitucionais, são eles: Constituição Federal (BRASIL, 1988), Código Civil (BRASIL, 2002), Código do Consumidor (BRASIL, 1990), Lei de Cadastro Positivo (BRASIL, 2011) e o Marco Civil da Internet (BRASIL, 2014). Desse modo, constatou-se que cada dispositivo regulamentava o tema somente em seu âmbito de incidência, portanto, eram limitados, não sendo aplicáveis a qualquer caso, bem como não dispunham de regras gerais sobre o tema.

Tratou-se, ainda, especificamente sobre o tripé axiológico previsto no Marco Civil da Internet (BRASIL, 2014) e sobre a Lei Geral de Proteção de Dados Pessoais (BRASIL, 2018), destacando seu caráter específico sobre o ambiente digital. Nesse momento foram apresentados os principais conceitos, princípios e bases legais previstos na LGPD (BRASIL, 2018) que guardam relação com o tema dessa pesquisa, como os conceitos de dados pessoais e dados pessoais sensíveis, banco de dados, titular, tratamento e consentimento, o princípio da transparência e base legal do consentimento. Ademais, tratou-se das normas que se referem as decisões automatizadas e ao *profiling*. Concluiu-se que a LGPD (BRASIL, 2018) apresenta normas e princípios a serem seguidas para que o processo de tratamento de dados seja feito de forma adequada.

Assim, dispõe a LGPD (BRASIL, 2018), como já tinha sido feito de maneira mais geral pelo Marco Civil da Internet (BRASIL, 2014), sobre a necessidade do instrumento expresso de consentimento como requisito de validade do tratamento de dados. No entanto, a título de crítica inicial, destacou-se a contradição dos mecanismos legais vigentes com uma leitura mais correta do princípio da transparência, uma vez que para o consentimento ser válido deve se observar o princípio da transparência.

Por último, constatou-se que, em relação as decisões automatizadas, aos titulares dos dados colhidos cabe uma explicação em casos que se reconheça efeitos de divulgação de dados pessoais que acabem por ser realizada sem sua consulta ou conhecimento, praticamente de forma sub-reptícia, e por um processo de tomada de decisão automatizada. Em relação ao *profiling*, tal procedimento sequer é tratado pela LGPD (BRASIL, 2018) configurando um risco constante a privacidade e violação da transparência que decorre da mera lacuna legal.

Por fim, sobre o regime jurídico, cuidou-se de apresentar cinco projetos de lei que foram apresentados ao Congresso Nacional entre os anos de 2019 e 2021 que ainda se encontram em processo de tramitação legislativa, mas que já foram objeto de análise por especialistas da área do direito digital. Três dos cinco projetos apresentados tratam sobre a regulamentação da Inteligência Artificial no Brasil, um deles dispõe sobre a instituição de uma Lei brasileira de Liberdade, Responsabilidade e Transparência na Internet, que é voltada sobretudo para o combate da difusão de

Fake News no ambiente virtual, e, por último, tem-se um projeto de lei apresentado em 2020 que se propõe a disciplinar o uso de algoritmos na Internet, de modo a assegurar a transparência no uso de ferramentas que possam induzir as decisões tomadas na Internet.

No terceiro capítulo buscou-se demonstrar como ocorre o uso dos algoritmos pelas redes sociais e suas possíveis consequências a fim de identificar se há violação do princípio da transparência, bem como se a modulação algorítmica na sociedade brasileira realmente está acontecendo e quais seriam as consequências nocivas de tal prática. Nesse contexto, foi tratado com maior destaque sobre a técnica do *profiling* e a ausência ou mesma falta de efetividade dos controles de consentimento propostos na legislação em vigor.

Concluiu-se que o princípio da transparência, previsto no art. 6º, IV da LGPD (BRASIL, 2018) não é respeitado, uma vez que o consentimento é falho, ou seja, os usuários não leem as políticas de privacidade das redes sociais que estão se cadastrando, o consentimento é concedido de forma geral para todas as cláusulas da política de privacidade, sem a identificação de ato específico de divulgação ou mesmo delimitação temporal e material do que está se permitindo, portanto, contrário a previsão legal de que o consentimento deve se referir a finalidades determinadas. Além disso, somente é oportunizada a opção de concordar com os termos na forma de ato de adesão, que inclusive peca pela linguagem técnica, incapaz de configurar uma declaração de vontade real dos usuários, resultando em mero direcionamento da escolha de aderir ao documento que não é realmente lido ou compreendido.

Ademais, em razão da técnica do *profiling* os usuários são colocados em grupos conforme suas preferências, em uma bolha com filtros invisíveis, e, devido a vigilância ubíqua operada pelos aparelhos digitais conectados à Internet, estes mesmos usuários estão sob constante observação. Tal fenômeno permite a presença da modulação, operada pelos algoritmos, pois estes, vinculados as tecnologias da informação e da comunicação, são responsáveis por identificar padrões e predizer comportamentos futuros, retirando a autonomia dos usuários de escolherem quais assuntos querem acessar, uma vez que estes ficam presos dentro da bolha dos filtros,

sem ter consciência de que recebem somente conteúdos relacionados com suas preferências.

Ao final dessa pesquisa concluiu-se que: i) há violação do princípio da transparência, previsto no art. 6º, IV da LGPD (BRASIL, 2018), em relação a forma como é transmitida a informação para os indivíduos que desejam se cadastrar em uma rede social, pois o texto contido nas políticas de privacidade não atende a forma estabelecida em lei de que a informação deve ser clara, precisa e de fácil acesso; e, ii) a modulação algorítmica está presente na sociedade brasileira, na medida em que os indivíduos são colocados em bolhas virtuais criadas a partir da ação dos algoritmos em coletar suas informações e formarem um perfil comportamental baseado nos interesses e preferências desses indivíduos.

Além disso, no tocante ao regime jurídico brasileiro constatou-se que: iii) a legislação vigente no Brasil ainda não é suficiente para resolver o problema referente ao consentimento falho, bem como se mostra silente no que diz respeito a formação de perfis e admite a tomada de decisões unicamente automatizada que por sua própria natureza fere a exigência legal do consentimento prévio do usuário; e, iv) os Projetos de Lei, apesar de apresentarem algumas sanções, tratam de modo mais específico sobre a regulamentação da Inteligência Artificial e não estão suficientemente maduros para tratar do tema específico da violação de privacidade de usuário nas redes sociais, ou mesmo apresentam mecanismos efetivos que garantam a transparência do tratamento de dados.

Por fim, é necessário reconhecer que de todos os projetos apresentados, o que mais se aproxima do tema dessa pesquisa é o Projeto de Lei 4120/2020, pois trata de disciplinar o uso dos algoritmos. Entretanto, encontra-se atualmente arquivado. Consequentemente no presente momento não há uma norma, seja em vigor seja projetada, que trate especificamente sobre a regulamentação do uso dos algoritmos.

REFERÊNCIAS

AMARAL, Fernando. **Introdução à ciência de dados**. Rio de Janeiro: Alta Books, 2016.

ANTUNES, Deborah Christina; MAIA, Ari Fernando. **Big Data, exploração ubíqua e propagando dirigida:** novas facetas da indústria cultural. Psicologia USP. Instituto de Psicologia da Universidade de São Paulo, v. 29, n. 2, p. 189 – 199, 2018. Disponível em: https://repositorio.unesp.br/handle/11449/157663. Acesso em: 08. out. 2021.

BARRETO JÚNIOR, Irineu Francisco; CÉSAR, Daniel. Marco Civil da Internet e Neutralidade da rede: aspectos jurídicos e tecnológicos. **Revista Eletrônica do Curso de Direito da UFSM**. v. 12, n. 1, p. 65 – 88, 2017. Disponível em: https://periodicos.ufsm.br/revistadireito/article/view/23288. Acesso em: 21. mar. 2022.

BASTOS, Bruna; VON ENDE, Luiza Berger. O potencial de violação de direitos fundamentais no direcionamento de anúncios feito por algoritmos *online*. **Revista Ilustração**, Cruz Alta, v. 1, n. 3, set./dez., p. 19 – 29, 2020. Disponível em: https://www.editorailustracao.com.br/index.php/ilustracao/article/view/24. Acesso em: 14. dez. 2021.

BENTHAM, Jeremy. **O Panóptico ou a casa de inspeção**. In: BENTHAM, Jeremy; MILLER, Jacques-Alain; PERROT, Michelle; WERRETT, Simon. **O Panóptico.** org. Tomaz Tadeu; trad. Guacira Lopes Louro, 2. ed., Belo Horizonte: Autêntica, 2008.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais:** a função e os limites do consentimento. 3. ed., Rio de Janeiro: Forense, 2021.

BOTELHO, Marcos César. A proteção de dados pessoais enquanto direito fundamental: considerações sobre a Lei Geral de Proteção de Dados Pessoais. **Argumenta Journal Law.** Jacarezinho/PR, n. 32, jan./jun., p. 191 – 107, 2020. Disponível em: http://seer.uenp.edu.br/index.php/argumenta/article/view/1840. Acesso: 3. jan. 2022.

BRASIL. **Constituição da República Federativa do Brasil.** Senado Federal. Brasília, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 08. out. 2021.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 21, de 03 de fevereiro de 2020**. Estabelece fundamentos, princípios e diretrizes para o desenvolvimento e a aplicação da inteligência artificial no Brasil; e dá outras providências. Brasília: Câmara dos Deputados, 2020a. Disponível em: https://www.camara.leg.br/propostas-legislativas/2236340. Acesso em: 04. abr. 2022.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 2630, de 03 de julho de 2020**. Institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet.

Brasília: Câmara dos Deputados, 2020b. Disponível em: https://www.camara.leg.br/propostas-legislativas/2256735. Acesso em: 04. abr. 2022.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 4120, de 07 de agosto de 2020.** Disciplina o uso de algoritmos pelas plataformas digitais na internet, assegurando transparência no uso das ferramentas computacionais que possam induzir a tomada de decisão ou atuar sobre as preferências dos usuários. Brasília: Câmara dos Deputados, 2020c. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2259721. Acesso em: 04. abr. 2022.

BRASIL. Lei n. 8.078, de 11 de setembro de 1990. **Dispõe sobre a proteção do consumidor e dá outras providências**. (Código de Defesa do Consumidor). Diário Oficial da União. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 3. jan. 2022.

BRASIL. Lei n. 10.406, de 10 de janeiro de 2002. **Institui o Código Civil**. Diário Oficial da União. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 3. jan. 2022.

BRASIL. Lei n. 12.414, de 9 de junho de 2011. **Disciplina a formação e consulta a banco de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito**. (Lei de Cadastro Positivo). Diário Oficial da União. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 3. jan. 2022.

BRASIL. Lei n. 12.965, de 23 de abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.** (Marco Civil da Internet). Diário Oficial da União. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 08. out. 2021.

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Diário Oficial da União. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 08. out. 2021.

BRASIL. Lei n. 14.010, de 10 de junho de 2020. **Dispõe sobre o Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado (RJET) no período da pandemia do coronavírus (Covid-19).** Diário Oficial da União. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/L14010.htm. Acesso em: 3. jan. 2022.

BRASIL. Senado Federal. **Projeto de Lei nº 5051, de 16 de setembro de 2019**. Estabelece os princípios para o uso da Inteligência Artificial no Brasil. Brasília: Senado Federal, 2019. Disponível em:

https://www25.senado.leg.br/web/atividade/materias/-/materia/138790. Acesso em: 07. abr. 2022.

BRASIL. Senado Federal. **Projeto de Lei nº 872, de 12 de março de 2021**. Dispõe sobre o uso da Inteligência Artificial. Brasília: Senador Federal, 2021. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/147434. Acesso em: 07. abr. 2022.

BRUNO, Fernanda. Monitoramento, classificação e controle nos dispositivos de vigilância digital. **FAMECOS**. Porto Alegre, n. 36, ago., 2008. Disponível em: https://revistaseletronicas.pucrs.br/ojs/index.php/revistafamecos/article/view/4410. Acesso em: 11. jan. 2022.

BYTEDANCE. **TikTok**. China: 2016. Disponível em: https://www.tiktok.com/pt-BR/. Acesso em: 22. abr. 2022.

CASTELLS, Manuel. A era da informação: Economia, sociedade e cultura. **A Sociedade em rede**. v. 1. 14. ed., São Paulo: Paz e Terra, 2011.

CASTRO, Paulo César. Algoritmos devem ser debatidos. [Entrevista concedida a] Vitor Necchi. **Revista do Instituto Humanista Unisinos IHU ON-LINE**. São Leopoldo, ano XVI, ed. 495, p. 25 – 30, 2016. Disponível em: https://www.ihuonline.unisinos.br/edicoes-anteriores. Acesso em: 02. mar. 2022.

CHEVITARESE, Leandro; PEDRO, Rosa Maria Leite Ribeiro. Da Sociedade Disciplinar à Sociedade de Controle: a questão da liberdade por uma alegoria de Franz Kafka, em *O Processo* e de Phillip Dick, em *Minority Report*. In: Estudos de Sociologia. **Revista do Programa de Pós-graduação em Sociologia da UFPE**, Recife, v. 8, n. 1 e 2, p. 129 – 162, 2005. Disponível em: http://clareira.com.br/wp-content/uploads/2017/09/A-Quest%C3%A3o-da-liberdade-vers%C3%A3o-for-publish.pdf. Acesso em: 10. jan. 2022.

COLNAGO, Cláudio de Oliveira Santos. **Liberdade de Expressão na Internet:** Desafios regulatórios e parâmetros de interpretação. 2016. 208 f. Doutorado em direito – Faculdade de Direito de Vitória, Vitória/ES, 2016.

CONSELHO DA JUSTIÇA FEDERAL. Enunciado 404. **V Jornada de Direito Civil**. Brasília, 2012. Disponível em: https://www.cjf.jus.br/cjf/corregedoria-da-justica-federal/centro-de-estudos-judiciarios-1/publicacoes-1/jornadas-cej/vjornadadireitocivil2012.pdf. Acesso em: 13. abr. 2022.

COSTA, Rogério da. Sociedade de Controle. **São Paulo em Perspectiva**. São Paulo, v. 18, n. 1, p. 161 – 167, mar., 2004. Disponível em: https://www.scielo.br/j/spp/a/ZrkVhBTNkzkJr9jVw6TygVC/abstract/?lang=pt. Acesso em: 13. jan. 2022.

DELEUZE, Gilles. Post-scriptum sobre as sociedades de controle. In: DELEUZE, Gilles. **Conversações**. Tradução de Peter Pál Pelbart. São Paulo: Editora 34,1992, p. 219 - 226.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: fundamentos da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Revista dos Tribunais, 2020.

DONEDA, Danilo. Princípios e proteção de dados. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). **Direito e Internet III:** marco civil da internet. São Paulo: Quartier Latin, 2015.

FORGIONI, Paula Andrea; MIURA, Maira Yuriko Rocha. O princípio da neutralidade e o marco civil da *Internet* no Brasil. In: Newton de Lucca; Adalberto Simão Filho; Cíntia Rosa Pereira de Lima. (Org.). Direito e Internet III, 1. ed., n. 4, São Paulo: Quartier Latin, 2015.

FOUCAULT, Michel. **Vigiar e Punir**: nascimento da prisão, trad. Raquel Ramalhete, 20. ed. Petrópolis/RJ: Vozes, 1999.

FUCHS, Christian. **Social Media**: a critical introduction. 1. ed., Sage Publications, 2014.

GAGLIANO, Pablo Stolze; PAMPLONA FILHO, Rodolfo. **Novo curso de direito civil**: contratos, teoria geral. v. 4, tomo I. 13. ed. São Paulo: Saraiva, 2017.

GARCIA, José Wilson Correa. Sociabilidade Algorítmica: o desafio de não perdermos a humanidade que nos une pela polaridade que nos divide na era da Internet. **Revista do Instituto Humanista Unisinos IHU ON-LINE**. Rio Grande do Sul, 2020. Disponível em: https://www.ihu.unisinos.br/78-noticias/595489-sociabilidade-algoritmica-o-desafio-de-nao-perdermos-a-humanidade-que-nos-une-pela-polaridade-que-nos-divide-na-era-da-internet#. Acesso em: 02. mar. 2022.

GARCIA, Rebeca. Marco Civil da Internet no Brasil: repercussões e perspectivas. **Revista dos Tribunais**. São Paulo, v. 964, fev., 2016. Disponível em: https://dspace.almg.gov.br/handle/11037/20729. Acesso em: 17. mar. 2022.

GAMBA, João Roberto Gorini. Breves Notas sobre os impactos políticos e jurídicos causados pelas redes sociais. **GenJurídico**. 2021. Disponível em: http://genjuridico.com.br/2021/10/13/redes-sociais-impactos-politicos/. Acesso em: 02. mar. 2022.

GILLESPIE, Tarleton. The relevance of algorithms. *In*: GILLESPIE, Tarleton; BOCZKOWSKI, Pablo J.; FOOT, Kirsten A. **Media technologies**: Essays on communication, materiality, and society. MIT Press, 2014. Disponível em: https://mitpress.universitypressscholarship.com/view/10.7551/mitpress/9780262525374.001.0001/upso-9780262525374-chapter-9. Acesso em: 08. out. 2021.

HAN, Byung-Chul. **Sociedade da Transparência**. Rio de Janeiro: Vozes, 2017.

HARARI, Yuval Noah. **21 lições para o século 21**. São Paulo: Companhia das Letras, 2018.

HOFFMANN-RIEM, Wolfgang. Controle do Comportamento por Meio de Algoritmos: um Desafio para o Direito. **Revista Direito Público**. *[S.l.].* v. 16, 2019. Disponível

em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3647. Acesso em: 16. mar. 2022.

KOWALSKI, Robert. Algorithm = logic + control. ***Communications of the ACM***, v. 22, n.7, 424–435, 1979. Disponível em: https://www.doc.ic.ac.uk/~rak/papers/algorithm%20=%20logic%20+%20control.pdf. Acesso em: 08. out. 2021.

LEITÃO, Nicolas Samuel Gomes; SOARES, Telmir de Souza. **Modulação Deleuziana, Modulação Algorítmica e Manipulação Midiática na Sociedade de Controle**. In: II Semana Nacional de Teologia, Filosofia e Estudos de Religião e II Colóquio Filosófico. Mossoró/RN, 2021, p. 160 – 168. Disponível em: https://www.doity.com.br/anais/semana-nacional-teo-filos-e-cr/trabalho/178640. Acesso em: 08. out. 2021.

LIMA, Clarissa Fernandes de. O *profiling* e a proteção de dados pessoais. 2019, 81 f. Trabalho de Conclusão de Curso (Bacharel) – Faculdade de Direito da Universidade Federal do Rio Grande do Sul, Porto Alegre, 2019. Disponível em: https://lume.ufrgs.br/handle/10183/199951. Acesso em: 02. abr. 2022.

LIMA, Taísa Maria Macena; SÁ, Maria de Fátima Freire de. Inteligência Artificial e Lei Geral de Proteção de Dados Pessoais: o direito à explicação nas decisões automatizadas. **Revista Brasileira de Direito Civil**, Belo Horizonte, v. 26, p. 227 – 246, out./dez., 2020. Disponível em: https://rbdcivil.ibdcivil.org.br/rbdc/article/view/584. Acesso em: 02. abr. 2022.

LONGHI, João Vitor Rozatti. Marco Civil da Internet no Brasil: breves considerações sobre seus fundamentos, princípios e análise crítica do regime de responsabilidade civil dos provedores. In: SOUZA, Allan Rocha de; [et al]. **Direito Digital:** Direito Privado e Internet. org. Guilherme Magalhães Martins, João Vitor Rozatto Linghi. 3. ed. São Paulo: Editora Foco, p. 115 – 144, 2020.

LUGATI, Lys Nunes; ALMEIDA, Juliana Evangelista de. Da evolução das legislações sobre proteção de dados: a necessidade de reavaliação do papel do consentimento como garantidor da autodeterminação informativa. **Revista de Direito**. V. 12, n. 02, p. 01 – 33, 2020. Disponível em: https:/periodicos.ufv.br/revistadir/article/view/10597. Acesso em: 12. abr. 2022.

MARTELETO, Regina Maria. Análise de redes sociais: aplicação nos estudos de transferência da informação. **Ciência da Informação**. Brasília, v. 30, n. 1, p. 71 – 81, jan./abr., 2001. Disponível em: http://revista.ibict.br/ciinf/article/view/940. Acesso em: 08. out. 2021.

MARTELETO, Regina Maria. Redes sociais, mediação e apropriação de informações: situando campos, objetos e conceitos na pesquisa em Ciência da Informação. **Tendências da Pesquisa Brasileira em Ciência da Informação**, Brasília, v. 3, n.1, p. 27 – 46, jan./ dez., 2010. Disponível em: https://www.arca.fiocruz.br/handle/icict/2247. Acesso em: 08. out. 2021.

MAYER-SCHONBERGER, Viktor; CUKIER, Kenneth. **Big data:** como extrair volume, variedade, velocidade e valor da avalanche de informação cotidiana. Tradução Paulo Polzonoff Junior. Rio de Janeiro: Elsevier, 2013.

MENEZES NETO, Elias Jacob de; MORAIS, Jose Luis Bolzan de. Análises Computacionais Preditivas como um novo biopoder: Modificações do tempo na sociedade dos sensores. **Novos Estudos Jurídicos**, v. 24, n. 3, set./dez., p. 1129 – 1153, 2018. Disponível em: https://siaiap32.univali.br/seer/index.php/nej/article/view/13769. Acesso em: 14. mar. 2022.

META. **Instagram**. Estados Unidos da América: 2010. Disponível em: https://www.instagram.com/. Acesso em: 22. abr. 2022.

MONTEIRO, Edgard. Fake News, PL 2630/20, Liberdade de Expressão e Informação. Não deixe que tentem te confundir. **Jusbrasil**, 2020. Disponível em: https://edge2m.jusbrasil.com.br/artigos/853778536/fake-news-pl-2630-20-liberdade-de-expressao-e-de-informacao-nao-deixe-que-tentem-te-confundir. Acesso em: 13. abr. 2022.

MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da Lei Geral de Proteção de Dados (Lei 13.709/18). **Revista de Direitos e Garantias Fundamentais**, Vitória/ES, v. 19, n. 3, set./dez., p. 159 – 180, 2018. Disponível em: https://sisbib.emnuvens.com.br/direitosegarantias/article/view/1603. Acesso em: 16. dez. 2021.

NOGUEIRA, Roberto Henrique Pôrto; ESTÊVES, Guilherme Mesquita. Relações Negociais envolvendo dados pessoais, boa-fé objetiva e análise econômica do direito. **Empório do Direito**. 2020. Disponível em: https://emporiododireito.com.br/leitura/relacoes-negociais-envolvendo-dados-pessoais-boa-fe-objetiva-e-analise-economica-do-direito. Acesso em: 08. maio. 2022.

PARISER, Eli. **O filtro invisível**: o que a internet está escondendo de você. 1. ed., Rio de Janeiro, Zahar, 2012.

PELLIZZARI, Bruno Henrique Miniuchi; BARRETO JUNIOR, Irineu Francisco. Bolhas Sociais e seus efeitos na sociedade da informação: ditadura do algoritmo e entropia na internet. **Revista de Direito, Governança e Novas Tecnologias**, Belém, v.5, n.2, jul./dez., p. 57 – 73, 2019. Disponível em: https://indexlaw.org/index.php/revistadgnt/article/view/5856. Acesso em: 08. out. 2021.

PONTIERI, Alexandre. Marco Civil da Internet: Neutralidade de rede e Liberdade de expressão. **Migalhas**, 2018. Disponível em: https://www.migalhas.com.br/depeso/284816/marco-civil-da-internet---neutralidade-de-rede-e-liberdade-de-expressao. Acesso em: 21. mar. 2022

RAEFFRA, Ana Paula Oriola de; SANTOS, Jhoni de Sousa Medrado dos. A prorrogação do prazo de vigência da lei geral de proteção de dados pessoais: LGPD e seus impactos no desenvolvimento econômico do Brasil diante da pandemia. **Migalhas**, 2020. Disponível em: https://www.migalhas.com.br/depeso/325364/a-prorrogacao-do-prazo-de-vigencia-da-lei-geral-de-protecao-de-dados-pessoais---lgpd-e-seus-impactos-no-desenvolvimento-economico-do-brasil-diante-da-pandemia. Acesso em: 25. abr. 2022.

REIS, Émilien Vilas Boas; NAVES, Bruno Torquato de Oliveira. O meio ambiente digital e o direito à privacidade diante do *big data*. **Veredas do Direito**. Belo Horizonte/MG, v. 17, n. 37, jan./abr., p. 145 – 167, 2020. Disponível em: http://revista.domhelder.edu.br/index.php/veredas/article/view/1795. Acesso em: 11. jan. 2022.

RIPARI, César. Por que dados são considerados o novo Petróleo. **INFRAROI.** 2019. Disponível em: https://infraroi.com.br/por-que-dados-sao-considerados-o-novo-petroleo/. Acesso em: 07. maio. 2022.

ROSSETTI, Regina; ANGELUCI, Alan. Ética Algorítmica: questões e desafios éticos do avanço tecnológico da sociedade da informação. **Galáxia**. São Paulo, online, ISSN: 1982-2553, Publicação Contínua, n. 46, p. 1 – 18, 2021. Disponível em: https://revistas.pucsp.br/index.php/galaxia/article/view/50301. Acesso em: 12. jan. 2022.

RUIZ, Castor M. M. Bartolomé. Os dispositivos de poder da sociedade de controle e seus modos de subjetivação. In: **Revista de Filosofia Unisinos**. São Leopoldo, v. 5, n. 9, jul./dez., p. 63 – 100, 2004. Disponível em: http://revistas.unisinos.br/index.php/filosofia/article/view/6549. Acesso em: 18. jan. 2022.

SANTA ROSA, Giovanni. Lei da inteligência artificial no Brasil: entenda o projeto aprovado na Câmara. **Tecnoblog**. 2021. Disponível em: https://tecnoblog.net/especiais/lei-da-inteligencia-artificial-no-brasil-entenda-o-projeto-aprovado-na-camara/. Acesso em: 13. abr. 2022.

SARTORI, Ellen Carina Mattias; BAHIA, Cláudio José Amaral. Big Brother is watching you: da distopia orwelliana ao direito fundamental à proteção de dados pessoais. **Revista de Direito e Garantias Fundamentais.** v. 20, n. 3, p. 225 – 248, set./dez., Vitória/ES, 2019. Disponível em: https://sisbib.emnuvens.com.br/direitosegarantias/article/view/1785. Acesso em: 16. dez. 2021.

SIQUEIRA JÚNIOR, Paulo Hamilton. Direito Informacional: direito da sociedade da informação. **Revista dos Tribunais**, São Paulo, v. 96, n. 859, maio, p. 1 - 16, 2007. Disponível em: https://dspace.almg.gov.br/handle/11037/28841. Acesso em: 08. out. 2021.

SIQUEIRA JÚNIOR, Paulo Hamilton. **Teoria do direito**. São Paulo: Saraiva, 2009.

SILVA, Luanna Angélica. **Marco Civil da Internet e o princípio da neutralidade da rede**. 2018. 66 f. Monografia (Graduação em Direito) – Universidade Federal Rural do Semi-árido (UFERSA), Mossorô/RN, 2018. Disponível em: https://repositorio.ufersa.edu.br/bitstream/prefix/3438/2/LuanaAS_MONO.pdf. Acesso em: 04. abr. 2022.

SILVA, Vanessa Junior da. **Proteção Geral de Dados**: Comunidade Europeia X Brasil. 2019. 80 f. Monografia (Graduação em Direito) – Universidade do Vale do Taquari (UNIVATES), Lajeado, 2019. Disponível em: https://www.univates.br/bdu/bitstream/10737/2796/1/2019VanessaJuniordaSilva.pdf. Acesso em: 09. abr. 2022.

SILVEIRA, Sérgio Amadeu da. **Democracia e os códigos invisíveis**: como os algoritmos estão modulando comportamentos e escolhas políticas. Edições Sesc: São Paulo. 2019.

SILVEIRA, Sérgio Amadeu da. Discurso sobre Regulação e Governança Algorítmica. **Estudos de Sociologia** [S.l], v. 25, n. 48, jan./ jun., p. 63 – 85, 2020. DOI: 10.52780/res. 13530. Disponível em: https://periodicos.fclar.unesp.br/estudos/article/view/13530. Acesso: 08. out. 2021.

SILVEIRA, Sérgio Amadeu da. **A noção de modulação e os sistemas algorítmicos**. In: SOUZA, Joyce; AVELINO, Rodolfo; SILVEIRA, Sérgio Amadeu da. A sociedade de controle: manipulação e modulação nas redes sociais. 2. ed., p. 33 – 47, São Paulo: Hedra, 2021.

SOUSA, Jéffson Menezes de. **A efetividade da proteção de dados pessoais frente ao *big data***. 2017. 111 f. Dissertação (Mestrado) - Curso de Mestrado em Direitos Humanos, Programa de Pós-Graduação em Direito, Universidade Tiradentes, Aracaju, 2017. Disponível em: https://mestrados.unit.br/wp-content/uploads/sites/5/2017/06/A-EFETIVIDADE-DA-PROTE%C3%87%C3%83O-DE-DADOS-PESSOAIS.pdf. Acesso em: 08. out. 2021.

SOUSA, Jéffson Menezes de; OLIVEIRA, Liziane Paixão Silva. Banco de dados automatizados: a versão “ciberespacial” do panóptico na sociedade de controle. **Revista Jurídica Luso-Brasileira – RJLB**. Ano 6, n. 2, p. 613 – 637, 2020. Disponível em: https://www.cidp.pt/revistas/rjlb/2020/2/2020_02_0000_CAPA.pdf. Acesso em: 11. jan. 2022.

SOUZA, Joyce; AVELINO, Rodolfo; SILVEIRA, Sérgio Amadeu da. **A modulação de opiniões e comportamento**. In: SOUZA, Joyce; AVELINO, Rodolfo; SILVEIRA, Sérgio Amadeu da. A sociedade de controle: manipulação e modulação nas redes sociais. 2. ed., p. 9 – 11, São Paulo: Hedra, 2021.

SOUZA, Renato Rocha. Sobre a ética humana e a ética dos algoritmos. P. 577 – 586. In: org. REIA, Jhessica; FRANCISCO, Pedro Augusto P.; BARROS, Marina; MAGRANI, Eduardo. **Horizonte Presente**: Tecnologia e Sociedade em debate. Belo Horizonte: Casa do Direito; FGV – Fundação Getúlio Vargas, 2019.

TAKAHASHI, Tadao (Org.). **Sociedade da Informação no Brasil:** livro verde. Brasília: Ministério da Ciência e Tecnologia, 2000. Disponível em: https://livroaberto.ibict.br/handle/1/434. Acesso em: 08. out. 2021.

TAVARES, Bárbara L. Consciência e liberdade na era do big data: paradigmas do sujeito contemporâneo. **Guairacá Revista de Filosofia**. Guarapuava/PR, v. 35, n. 1, p. 133 – 152, 2019. Disponível em: 19. jan. 2022.

TEFFÉ, Chiara Spadaccini de; MORAES, Maria Celina Bodin de. Redes sociais virtuais: privacidade e responsabilidade civil Análise a partir do Marco civil da Internet. **Pensar:Revista de Ciências Jurídicas**. Fortaleza, v. 22, n. 1, p. 108 – 146, jan./abr., 2017. Disponível em: https://periodicos.unifor.br/rpen/article/view/6272. Acesso em: 21. mar. 2022.

TEIXEIRA, Bruno Costa. **Cidadania em rede:** A inteligência coletiva enquanto potência recriadora da democracia participativa. 2012. 130 f. Mestrado em direitos e Garantias Fundamentais – Faculdade de Direito de Vitória, Vitória/ES, 2012.

TEIXEIRA, Tarcisio; ARMELIM, Ruth Maria Guerreiro da Fonseca. **Lei Geral de Proteção de Dados Pessoais:** Comentada artigo por artigo. 3. ed. ver., atual. e ampl., Salvador: Editora JusPodivm, 2021.

TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. O consentimento na circulação de dados pessoais. **Revista Brasileira de Direito Civil**. Belo Horizonte/MG, v. 25, jul./set., p. 83 – 116, 2020. Disponível em: https://rbdcivil.ibdcivil.org.br/rbdc/article/view/521. Acesso em: 27. dez. 2021.

THE ECONOMIST. The world's most valuable resource is no longer oil, but data. 2017. Disponível em: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data. Acesso em: 24. mar. 2022.

TOMAÉL, Maria Inês; ALCARÁ, Adriana Rosecler; DI CHIARA, Ivone Guerreiro. Das redes sociais à inovação. **Ciência da Informação.** Brasília, v. 34, n. 2, maio/ago., p. 93 – 104, 2005. Disponível em: https://www.scielo.br/j/ci/a/WTMRGVXjNdLNLDwGBD5HTXb/abstract/?lang=pt. Acesso em: 27. dez. 2021.

TWITTER INC. **Twitter**. Estados Unidos da América: 2006. Disponível em: https://twitter.com/. Acesso em: 22. abr. 2022.

UNIÃO EUROPEIA. Conselho da Europa. **Convenção nº 108**. 1981.

UNIÃO EUROPEIA. Parlamento e Conselho. **Diretiva 95/46/CE**, de 24 de outubro de 1995. Relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Jornal Oficial da União Europeia. L 281, 23 nov. 1995. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046. Acesso em: 15. abr. 2022.

UNIÃO EUROPEIA. ***General Data Protection Regulation*** (Regulamento Geral sobre Proteção de Dados). 2016. Disponível em: https://gdprinfo.eu/pt-pt. Acesso em: 15. abr. 2022.

UNIÃO EUROPEIA. Parlamento e Conselho. **Regulamento (EU) 2016/679**, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Jornal Oficial da União Europeia. L 119/1, 4 maio 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 15. abr. 2022.

VERMELHO, Sônia Cristina; VELHO, Ana Paula Machado; BONKOVOSKI, Amanda; PIROLA, Alisson. Refletindo sobre as redes sociais digitais. **Educação e Sociedade**, Campinas, v. 35, n. 126, jan./ mar., p. 179 – 196, 2014. Disponível em: https://www.scielo.br/j/es/a/4JR3vpJqszLSgCZGVr88rYf/abstract/?lang=pt. Acesso em: 08. out. 2021.

VIDAL JÚNIOR, Ícaro Ferraz. Como os algoritmos definem o que você vê no Facebook e no Google. [Entrevista concedida a] Leyberson Pedrosa. **Revista do Instituto Humanista Unisinos IHU ON-LINE**. Rio Grande do Sul, 2016. Disponível em: https://www.ihu.unisinos.br/78-noticias/556660-como-os-algoritmos-definem-o-que-voce-ve-no-facebook-e-no-google. Acesso em: 02. mar. 2022.

ZANATTA, Rafael A. F. **Perfilização, Discriminação e Direitos: do Código de Defesa do Consumidor à Lei Geral de Proteção de Dados Pessoais**. Universidade de São Paulo, São Paulo, 2019. Disponível em: https://www.researchgate.net/publication/331287708_Perfilizacao_Discriminacao_e_Direitos_do_Codigo_de_Defesa_do_Consumidor_a_Lei_Geral_de_Protecao_de_Dados_Pessoais. Acesso em: 21. abr. 2022.