

**UNIVERSIDADE FEDERAL DE JUIZ DE FORA**  
**FACULDADE DE DIREITO**  
**PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO**

**Pâmela Marchese Braga**

**Vigilância Algorítmica:** a datificação da personalidade e sua proteção  
legislativa

Juiz de Fora  
2023

**Pâmela Marchese Braga**

**Vigilância Algorítmica:** a datificação da personalidade e sua proteção legislativa

Dissertação apresentada ao Programa de Pós-Graduação em Direito da Faculdade de Direito da Universidade Federal de Juiz de Fora, como requisito parcial para obtenção do grau de Mestra no Mestrado em Direito e Inovação.

Orientador: Prof. Dr. Sergio Marcos Carvalho de Ávila Negri.

Juiz de fora

2023

Ficha catalográfica elaborada através do programa de geração automática da Biblioteca Universitária da UFJF, com os dados fornecidos pelo(a) autor(a)

Marchese Braga, Pâmela .

Vigilância Algorítmica: : a datificação da personalidade e sua proteção legislativa / Pâmela Marchese Braga. -- 2023.  
115 f.

Orientador: Sergio Marcos Carvalho de Ávila Negri  
Dissertação (mestrado acadêmico) - Universidade Federal de Juiz de Fora, Faculdade de Direito. Programa de Pós-Graduação em Direito, 2023.

1. Daditificação. 2. Privacidade. 3. Profiling. 4. Proteção de dados. 5. Vigilância . I. Marcos Carvalho de Ávila Negri, Sergio , orient. II. Título.

**Pâmela Marchese Braga**

**Vigilância Algorítmica:** a datificação da personalidade e sua proteção legislativa

Dissertação apresentada  
ao Programa de Mestrado  
em  
Direito da Universidade  
Federal de Juiz de Fora  
como requisito parcial à  
obtenção do título de  
Mestre em Direito. Área  
de concentração: Direito e  
Inovação

Aprovada em 15 de abril de 2024

**BANCA EXAMINADORA**

**Sergio Marcos Carvalho de Avila Negri - Orientador**  
Universidade Federal de Juiz de Fora

**Wagner Silveira Rezende**  
Instituição

**Elora Raad Fernandes**  
Instituição

Juiz de Fora, 12/04/2024.



Documento assinado eletronicamente por **Sergio Marcos Carvalho de Avila Negri, Professor(a)**, em 22/05/2024, às 16:04, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Wagner Silveira Rezende, Professor(a)**, em 22/05/2024, às 16:27, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).

---



Documento assinado eletronicamente por **Elora Raad Fernandes, Usuário Externo**, em 14/07/2024, às 05:57, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).

---



Documento assinado eletronicamente por **Pâmela Marchese Braga, Usuário Externo**, em 16/07/2024, às 18:24, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).

---



A autenticidade deste documento pode ser conferida no Portal do SEI-Ufjf ([www2.ufjf.br/SEI](http://www2.ufjf.br/SEI)) através do ícone Conferência de Documentos, informando o código verificador **1780419** e o código CRC **9F2F5079**.

---

Dedico este trabalho à minha mãe  
por seu apoio e paciência.

## **AGRADECIMENTOS**

Agradeço, primeiramente, à minha mãe, Selma, pelo constante apoio, amor e amparo durante essa etapa.

Ao Centro Universitário Faminas Muriaé, faculdade onde me graduei, e em especial à coordenadora do curso de Direito, Margarida Espósito, pelo apoio e incentivo.

Agradeço ao meu orientador do Programa de Pós-graduação, Sérgio Negri, pela oportunidade de orientação e conhecimentos compartilhados.

Agradeço à Universidade Federal de Juiz de Fora (UFJF), à Faculdade de Direito da UFJF, ao Programa de Pós-graduação Stricto Sensu em Direito e Inovação da UFJF e à Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), pelas portas abertas e incentivo ao desenvolvimento acadêmico que me possibilitou chegar até aqui.

Agradeço, também, aos professores do programa e colegas que participaram da minha jornada acadêmica, ainda que de forma virtual, em razão da pandemia, propiciaram trocas valiosas.

Por fim, agradeço a todos os caminhos que me levaram à esta jornada.

## RESUMO

Os desdobramentos sociais da inovação, das comunicações e informações conduziram a sociedade para o atual cenário de hiperconexão, e consequentemente, com excessivo fluxo de dados, os indivíduos foram submetidos a um processo de digitalização de suas informações pessoais. Essa datificação da personalidade é decorrente do impacto das novas tecnologias em virtude da excessiva exposição à internet, e pode ocasionar riscos individuais no que se refere aos direitos personalíssimos, e públicos, quando se importa com o desenvolvimento da democracia a partir do impacto nos padrões de consumo de produtos, serviços e informações. As movimentações sociais exigem, consequentemente, um olhar jurídico sobre as novas temáticas tecnológicas, para que se contribua às discussões existentes, buscando agregar conhecimento aos estudos já elaborados na área, e compreender como se dá a vigilância e suas discriminações promovidas por algoritmos sobre os usuários da internet e de tecnologias inteligentes. Este estudo, então, teve por objetivo investigar se as legislações vigentes no Brasil seriam capazes de proteger os direitos personalíssimos desses usuários frente à toda obscuridade da atuação algorítmica. Para isso, foram utilizados métodos de pesquisa com análise qualitativa-exploratória partindo dos conceitos de privacidade de Rodotà e Doneda, e da datificação da personalidade de Mayer-Schoenberger e Cukier, passando por leituras de uma ampla biografia do Direito Digital e tecnológico, e uma investigação acerca da eficiência da legislação brasileira regulatória da temática. Inicialmente, foram levantadas hipóteses de que, i) existiriam pontos cegos legislativos sobre a regulamentação dos algoritmos nas questões de vigilância e, de que ii) havendo enquadramento regulatório, haveria dificuldades de aplicação e fiscalização normativas. A conclusão do presente trabalho é de que não existem regulamentações vigentes no ordenamento brasileiro, que sejam capazes de delinear a vigilância e discriminações algorítmicas, sendo necessário pensá-las apesar de toda a complexidade envolvida.

**Palavras-chave:** Datificação. Privacidade. Profiling. Proteção de dados. Vigilância.

## **ABSTRACT**

The social consequences of communications and information innovation have led society to the current scenario of hyperconnection, and consequently, with excessive flow of data, individuals have been subjected to a process of digitizing their personal information. This datafication of personality is due to the impact of new technologies due to excessive exposure to the internet, and can cause individual risks with regard to very personal and public rights, when it comes to the development of democracy based on the impact on standards of consumption of products, services and information. Social movements consequently block a legal look at new technological themes, so that it contributes to existing discussions, seeking to add knowledge to studies already modified in the area, and understand how surveillance and its discrimination promoted by algorithms on users takes place. the internet and smart technologies. This study, then, aimed to investigate whether the legislation in force in Brazil would be capable of protecting the very personal rights of these users in the face of all the obscurity of algorithmic action. For this, research methods were used with qualitative-exploratory analysis starting from the privacy concepts of Rodotà and Doneda, and the datafication of the personality of Mayer-Schoenberger and Cukier, going through readings of a broad biography of Digital and technological Law, and a investigation into the efficiency of Brazilian regulatory legislation on the subject. Initially, hypotheses were raised that, i) there would be legislative blind spots regarding the regulation of algorithms in surveillance issues and, that ii) having a regulatory framework, there would be difficulties in applying and supervising regulations. The conclusion of this work is that there are no current regulations in the Brazilian system that are capable of outlining surveillance and algorithmic discrimination, and it is necessary to think about them despite all the complexity involved.

**Keywords:** Datafication. Data protection. Privacy. Profiling. Surveillance.

## LISTA DE ABREVIATURAS E SIGLAS

|            |                                                                           |
|------------|---------------------------------------------------------------------------|
| AI         | <i>Artificial Intelligence</i>                                            |
| ARPANet    | <i>Advanced Research Project Agency Network</i>                           |
| Art.       | Artigo                                                                    |
| CDC        | Código de Defesa do Consumidor                                            |
| CJSUBIA    | Comissão de Juristas – PL n.º 2338/2023                                   |
| CRT        | <i>Cognitive Reflection Test</i>                                          |
| EAG        | <i>Ethics Advisory Group</i>                                              |
| FCC        | Federation Communications Commission                                      |
| GDPR       | <i>General Data Protection Regulation</i>                                 |
| IA         | Inteligência artificial                                                   |
| IOS        | <i>iPhone Operating System</i>                                            |
| IoT        | <i>Internet of things</i>                                                 |
| LGPD       | Lei Geral de Proteção de Dados                                            |
| LPI        | Lei de Propriedade Industrial                                             |
| MCI        | Marco Civil da Internet                                                   |
| MDB-PB     | Movimento Democrático Brasileiro – Partido do Brasil                      |
| n.º        | Número                                                                    |
| NSA        | <i>National Security Agency</i>                                           |
| OCDE       | Organização para a Cooperação e Desenvolvimento<br>Econômico ou Económico |
| p.         | Página                                                                    |
| PDT-CE     | Partido Democrático Trabalhista - Ceará                                   |
| Podemos-RN | Partido Político – Rio Grande do Norte                                    |
| PT         | Partido dos Trabalhadores                                                 |
| TCP        | <i>Transmission Control Protocol</i>                                      |
| TIC        | Tecnologias da Informação e Comunicação                                   |

## LISTA DE SÍMBOLOS

§ Parágrafo

% Porcentagem

## SUMÁRIO

|          |                                                                |            |
|----------|----------------------------------------------------------------|------------|
| <b>1</b> | <b>INTRODUÇÃO.....</b>                                         | <b>11</b>  |
| 1.1      | CONTEXTUALIZAÇÃO.....                                          | 12         |
| 1.2      | METODOLOGIA .....                                              | 16         |
| <b>2</b> | <b>INOVAÇÕES E SUAS IMPLICAÇÕES.....</b>                       | <b>22</b>  |
| 2.1      | AS COMUNICAÇÕES EM MASSA.....                                  | 25         |
| 2.2      | INFORMÁTICA E INTERNET.....                                    | 29         |
| 2.3      | O “NOVO” CONSUMIDOR.....                                       | 33         |
| <b>3</b> | <b>DATIFICAÇÃO DA PERSONALIDADE.....</b>                       | <b>38</b>  |
| 3.1      | INTERNET MÓVEL E MÍDIAS SOCIAIS.....                           | 40         |
| 3.2      | TECNOLOGIAS DE VIGILÂNCIA.....                                 | 44         |
| <b>4</b> | <b>VIGILÂNCIA ALGORÍTMICA.....</b>                             | <b>47</b>  |
| 4.1      | ALGORITMOS.....                                                | 49         |
| 4.2      | MINERAÇÃO DE DADOS E PERFIS.....                               | 53         |
| 4.3      | METADADOS – RASTROS DIGITAIS.....                              | 58         |
| 4.4      | CAPITALISMO DE VIGILÂNCIA: A ECONOMIA DA ATENÇÃO.....          | 60         |
| <b>5</b> | <b>CONSUMO DE INFORMAÇÕES POLÍTICAS E DESINFORMAÇÃO</b>        | <b>66</b>  |
| 5.1      | FAKE NEWS E DESINFORMAÇÃO.....                                 | 68         |
| 5.2      | RECEPTIVIDADE DAS NOTÍCIAS.....                                | 70         |
| 5.3      | CAMBRIDGE ANALYTICA – ESPIONAGEM POLÍTICA.....                 | 73         |
| 5.4      | ELEIÇÕES BRASILEIRAS – ASCENSÃO E QUEDA NA ERA<br>DIGITAL..... | 76         |
| <b>6</b> | <b>TECNOLOGIAS E OBSTÁCULOS À REGULAMENTAÇÃO.....</b>          | <b>81</b>  |
| 6.1      | LEGISLAÇÕES BRASILEIRAS NO DIGITAL.....                        | 82         |
| 6.2      | PROTEÇÃO DE DADOS PESSOAIS.....                                | 86         |
| 6.3      | GOVERNANÇA DOS ALGORÍTMOS.....                                 | 90         |
| 6.4      | IA E REGULAÇÃO.....                                            | 96         |
| <b>7</b> | <b>CONSIDERAÇÕES FINAIS.....</b>                               | <b>102</b> |
|          | <b>REFERÊNCIAS.....</b>                                        | <b>107</b> |

## INTRODUÇÃO

A pesquisa foi organizada em sete capítulos que buscam contextualizar o leitor sobre o cenário de inovações das comunicações em massa, sem aprofundar em detalhes históricos, mas buscando desenvolver a interpretação da autora de como se desenvolveu o contexto de vigilância e modificações nos padrões de consumo até que se chegasse ao que é hoje.

O primeiro capítulo é introdutório e apresenta resumidamente os métodos de pesquisa utilizados no desenvolvimento na pesquisa, como se deu sua organização em capítulos, e os fundamentos do estudo.

O segundo capítulo da pesquisa trata da temática do “*Inovações e suas implicações*” com uma contextualização acerca das comunicações em massa, o capítulo não busca se estender em questões históricas, mas inserir o leitor alheio ao tema, ao contexto da inovação tecnológica, especialmente a partir da narrativa de Tim Wu (2012) sobre inovações e de Bauman (2008, 2013) acerca do consumo, aproximando-o dos assuntos que serão discutidos nos capítulos seguintes. O capítulo se desenvolve dos primórdios da tecnologia, passando pelo surgimento da informática e internet, para que seja possível compreender como se deu o desenvolvimento da comunicação e consumo, até que se chegasse ao atual formato da internet e economia tecnológica.

No capítulo III, foi abordado a temática da “*Dadificação Da Personalidade*”, a partir do conceito de datificação da personalidade, concebido por Mayer-Schoenberger e Cukier (2013) e do perfil eletrônico abordado por Doneda (2019), o que é de extrema importância para a compreensão dos meios que possibilitaram à tecnologia uma interferência na esfera privada do indivíduo, colocando em risco seus direitos personalíssimos e o desenvolvimento da democracia e padrões de consumo econômicos e informacionais.

O quarto capítulo “*Vigilância algorítmica*”, se preocupa com as questões levantadas pela autora Cathy O’neil sobre os vieses algorítmicos e seu caráter discriminatório. Nesse tópico, serão abordadas questões conceituais de algoritmos de inteligência artificial (IA<sup>1</sup>). Além disso, o tópico fala sobre os metadados, que são dados residuais que deixam rastros dos usuários por onde

---

<sup>1</sup> O termo será aprofundado no tópico 4.1.

passam, e a possibilidade de se realizar a segmentação dos usuários da internet de acordo com seu perfil comportamental, tornando possível direcionar conteúdos de forma assertiva a pessoas ou grupos, e mais uma vez, violando a personalidade da pessoa humana.

No capítulo V, do “*Consumo de informações políticas e desinformação*”, são abordadas questões políticas sob a influência das inovações tecnológicas das redes sociais. A importância do tema se dá em razão da compreensão de que as manipulações existentes no contexto digital não ocorrem apenas na esfera do consumo de produtos e serviços, podendo, também, desenhar os caminhos da democracia sob influência de notícias falsas e desinformação. As contribuições de Shane (2019) sobre a forma como as notícias são percebidas pelo indivíduo foram de extrema importância para o desenvolvimento do tema.

O trabalho se desenvolve de forma a demonstrar os meios de afetação aos direitos personalíssimos do homem, frente às manipulações tecnológicas envoltas em técnicas de persuasão e *marketing*, que utilizam das emoções humanas na obtenção de resultados. Toda essa manipulação limita direitos como o da privacidade, proteção de dados, livre desenvolvimento da personalidade, uma vez que os usuários das tecnologias ficam expostos a uma rotina hiperconectada e de conteúdo manipulável.

No capítulo VI, “*Tecnologias e obstáculos à regulamentação*” é feita, então, uma abordagem sobre a sociedade atual, que vive hiperconectada e fornece a todo tempo, dados sobre si mesma, caracterizando o fenômeno do *Big Data*<sup>2</sup>.

Além disso, o capítulo discorre sobre a aplicação do direito às tecnologias inteligentes a partir de uma leitura legislativa das normativas do Direito Digital e proteção de dados no ordenamento jurídico brasileiro, governança algorítmica, personalidade eletrônica (Negri, 2020, 2021) e ética na robótica (Russel; Norvin, 2013), além da análise da eficiência do instituto do consentimento presente na LGPD<sup>3</sup> (Brasil, 2018), novo regulamento europeu de IA, e projetos de leis (PL<sup>4</sup>)

---

<sup>2</sup> Grande banco de dados que será abordado ao longo do texto.

<sup>3</sup> Lei Geral de Proteção de Dados, Lei nº 13.709 de 2018.

<sup>4</sup> Proposta normativa submetida ao processo legislativo brasileiro, uma espécie de anteprojeto de Lei.

sobre regulamentação da IA no Brasil (PL 21/2020 e PL 2238/23), na busca por uma mitigação nos vieses discriminatórios da inteligência artificial.

A pesquisa foi desenvolvida com um olhar lançado à vigilância, sem pretensão de esgotar a temática das implicações tecnológicas que recaem sobre ela, considerando as características e movimentações produzidas pelas tecnologias inteligentes e encarando o tema como um longo caminho a ser legalmente aperfeiçoado.

O trabalho foi pautado especialmente em questões de privacidade e proteção de dados, que há muito foram discutidas por Rodotà (2019) e Doneda (2019). A pesquisa não seguiu a linha de estudo aprofundado da LGPD ou do MCI<sup>5</sup>, pois o aspecto jurídico que se buscou estudar foi a preservação de garantias individuais e coletivas das personalidades datificadas frente à vigilância algorítmica. O que abrange questões muito além do que é regulamentado nos dispositivos de proteção de dados, sendo uma temática mais voltada a regulamentações das tecnologias inteligentes e invasivas.

Nas considerações finais, retoma-se as hipóteses levantadas: “i) *existiriam pontos cegos legislativos sobre a regulamentação dos algoritmos nas questões de vigilância e, de que ii) havendo enquadramento regulatório, haveria dificuldades de aplicação e fiscalização normativas*”, respondendo-as.

A primeira hipótese foi confirmada, uma vez que ainda não existe dispositivo vigente para regulamentação de sistemas inteligentes, contudo pontua-se que existe um projeto de lei caminhando para regular a temática; a segunda hipótese não pode ser confirmada por ausência de dispositivo legal, mas considerando uma análise sobre o PL 2238/23, acredita-se que existirão dificuldades de implementação na aplicação, podendo existir lacunas legislativas e tendo como agravante a incultura algorítmica, no sentido do desinteresse dos usuários de tecnologias em preservar seus direitos.

A pesquisa conclui como verdadeira, a primeira hipótese levantada e como possível a segunda hipótese se observada sobre o dispositivo que ainda se encontra em construção. Apesar disso, considera-se que pensar na regulamentação de IA no Brasil já é um grande avanço legislativo, entretanto as

---

<sup>5</sup> Marco Civil da Internet no Brasil, Lei nº 12.965 de 2014.

questões informáticas necessitam especialmente de conhecimento por parte de seus usuários, o que se apresenta como um fator agravante negativo.

## 1.1 CONTEXTUALIZAÇÃO

As comunicações em massa surgem, especialmente, com o rádio e a TV do século XX. A evolução tecnológica iniciou seu desenvolvimento sob moldes dos monopólios (Wu, 2012). Esse modelo econômico implica riscos à privacidade e ao livre desenvolvimento da personalidade, e mesmo em uma época de pouca tecnologia, em certa medida, influenciou o comportamento humano nos posicionamentos políticos e em sua inclinação ao consumismo, por meio das publicidades patrocinadas.

A então modificação drástica nos padrões de consumo, ou “revolução consumista”, foi o processo em que se transitou do consumo para o consumismo e as emoções do “consumir” passaram a sustentar a economia, isso porque a vida, para o consumo, é estar “em movimento” quando as ofertas estão sempre ultrapassadas, exigindo que se adquira o “novo”, (Bauman, 2008).

Nesse cenário, no início dos processos de inovação e tecnologia, o modelo de negócio publicitário fazia com que o indivíduo direcionasse sua atenção com uma finalidade econômica, sendo a atenção um meio de se alcançar o fim monetário, por exemplo, a partir de uma propaganda à qual prendeu sua atenção, adquiria-se um produto, gerando lucro para o contratante da publicidade transmitida na rádio ou na TV. Os anúncios na rádio se tornaram então, fonte de recursos para as estações transmissoras, que disputavam a atenção dos ouvintes, buscando alcançar maior audiência (Wu, 2012).

Posteriormente, surgem os computadores e depois a internet, e quando essas tecnologias se tornam acessíveis à grande massa, os contornos do consumo ganham nova perspectiva. Essa acessibilidade se torna exponencial através da popularização dos *smartphones*, mas as tecnologias *smarts*<sup>6</sup> se expandem para uma variedade de equipamentos além dos telefones móveis, e com isso, a internet adquire mobilidade e ubiquidade.

---

<sup>6</sup> Tecnologias com sistemas inteligentes (IA).

A aplicação da internet em dispositivos inteligentes que utilizam sensores e expõem o usuário a uma constante conexão, é conhecida por Internet das Coisas - IoT (Magrani, 2020).

Quando, então, a partir do amplo acesso tecnológico, o usuário empreende atenção extrema aos ambientes digitais, fornece um grande volume de informação sobre si mesmo, seus gostos e desgostos, opiniões políticas, o que lhe atrai ou lhe causa repulsa. Essas informações podem ser captadas enquanto esse indivíduo permanece conectado a algum aparelho de tecnologia *smart* que se encontre no ambiente, seja por meio de acesso a um site ou rede social, pela câmera, microfone ou imagens da galeria de um smartphone, ou até mesmo, georreferenciações.

Esta pesquisa faz uma leitura do usuário de internet enquanto consumidor, que ultrapassa o tradicional discurso consumerista, tratando também da absorção de informações, no sentido de se consumir, por exemplo, uma propaganda política, um artigo jornalístico ou até mesmo, uma notícia com conteúdo de desinformação, o que implica na manutenção do tempo comumente dedicado por um indivíduo ou grupo de pessoas a algum anúncio, considerando que a atenção sempre foi o combustível do *marketing* e as novas tecnologias são projetadas para atrair e monetizar a atenção dos usuários da internet.

É preciso compreender, então, que as temáticas do consumo, atenção, e vigilância se entrelaçam em razão de uma ser possibilitada pela outra. Essas possibilidades surgem a todo momento. A atenção de um usuário, assim como sua exposição por hiperconexão, alimentam a vigilância digital, e a partir desse mecanismo, as plataformas detêm extenso conhecimento, o que implica em controle e poder.

Dessa forma, a partir da hiperconexão, a personalidade é virtualizada e essa identidade digital do indivíduo contém amplo valor informacional, em razão dos dados coletados e, viabilizada pelo desenvolvimento e aprimoramento de tecnologias capazes de monitorar os hábitos de seus usuários, utilizando desse amplo conhecimento de perfil para persuadi-los a determinados comportamentos.

O mencionado excesso de exposição e utilização das plataformas digitais, aplicativos, *sites*, e demais meios de tecnologias digitais, permitem que sejam aplicadas técnicas comportamentais como o *profiling*, que é o perfilamento de

um indivíduo ou grupo de indivíduos, segmentando-os (*microtargeting*) a partir dos dados coletados e permitindo a identificação de hábitos e preferências, representando uma personificação virtual desses indivíduos (Doneda, 2019).

Compreende-se, então, que a sociedade passa por um momento de datificação da personalidade (Mayer-Schoenberger; Cukier, 2013), próprio da exposição excessiva a dispositivos conectados. Essa representação do “eu” em dados pessoais implica riscos às suas oportunidades e desenvolvimento pessoais (Bauman; Lyon, 2013).

Os riscos citados ou, em outras palavras, as possibilidades de controle e poder do “eu” por terceiros, se dão diariamente no consumo de produtos e serviços, mas também merecem atenção, as manipulações e desinformações favorecidas pelas tecnologias de vigilância.

Isso porque, toda a perfilação, previsão dos comportamentos e predileções, implicam em outras questões informacionais, o que é o caso do direcionamento de informações a partir da mineração de dados, com finalidade política (Bernardi, 2020).

Observa-se, que nos atuais modelos de negócios digitais a atenção do sujeito deixa de ser um meio, passando a ser o produto que gera recursos financeiros em si. Isso porque, o indivíduo empreende sua atenção no ambiente digital e é monitorado de diversas formas, possibilitando a identificação do seu perfil, seja consumerista ou político, e esse padrão obtido através da atenção dedicada pelo usuário de determinada plataforma digital, é o que será monetizado.

Atualmente, pode-se considerar a atenção como o fim em si mesma no que se refere à economia da atenção. Isso pois, a atenção em si tem valor de mercado, no que se refere ao modelo de negócios que promove a monetização dos dados pessoais, não dependendo em um primeiro momento da aquisição de produtos ou serviços, pois o que as tecnologias invasivas perseguem é conhecer os sentimentos e predileções dos indivíduos.

Em conjunto com toda essa vigilância, é aprimorado o que Shoshana Zuboff (2020) define como capitalismo de vigilância: um modelo de economia e consumo pertencentes à atual realidade digital, personalizados a partir da coleta de dados que é possibilitada pela experiência de conexão dos usuários, enquanto dedicam sua atenção às atividades nas plataformas digitais e na

utilização de dispositivos inteligentes. Isso permite que as empresas de tecnologia conheçam os hábitos de seus usuários, e monetizem esse “perfil” através da venda para outras empresas interessadas em conhecer esses consumidores.

Com toda essa previsibilidade de comportamento, permitida pelo conhecimento dos perfis dos usuários, as gigantes da tecnologia podem controlar tão profundamente seus usuários que se tornam capazes de prever seus comportamentos, como se realizassem uma leitura de seus pensamentos.

Essas técnicas, denominadas por *data mining* (mineração de dados) e aprimoradas por *data profiling* (perfil dos dados ou perfilamento), são possibilitadas em razão de algoritmos que trabalhavam com inteligência artificial, utilizando dados e metadados para conhecer o comportamento do usuário. Esses algoritmos são conhecidos por sua opacidade, que significa a dificuldade humana em visualizar e conhecer de forma clara sobre como se dá sua aplicação na coleta e tratamento de dados pessoais dos usuários das redes sociais.

Os metadados são informações residuais, podendo ser compreendidas como os “dados sobre dados”. As pessoas tendem a se preocupar apenas com o conteúdo de suas informações - como o que foi dito em uma conversa -, mas o que de fato se mostra relevante na manutenção da vigilância é o que está oculto nessas informações, como a geolocalização ou o tipo de equipamento utilizado para o envio das mensagens, nesses elementos reside o valor para compreender o perfil do usuário (Snowden, 2019).

A partir dessas informações, é possível segmentar os usuários individualmente ou em grupos e monetizar essas informações, como quando são vendidos anúncios que vão direcionar determinado conteúdo às pessoas com um perfil específico.

As sobreditas técnicas de segmentação e filtragem de dados, comprometem direitos personalíssimos constitucionais para além da própria privacidade e proteção de dados, mas comprometendo também, sua autonomia de decidir, por exemplo, sobre o que deseja visualizar nas redes sociais, prejudicando seu livre desenvolvimento, interferindo em suas decisões e prejudicando a democracia.

O grande volume de dados coletados pelas tecnologias é denominado de *Big Data*. Esses dados são coletados em uma grande velocidade e variedade

que supera qualquer outra tecnologia utilizada anteriormente para coleta e processamento de dados, bem como as capacidades de operação humanas (Bioni, 2021).

A partir das pesquisas realizadas e expostas sobre vigilância, visualiza-se a necessidade de regulamentar as tecnologias inteligentes e invasivas, isso em razão dos riscos à personalidade e aos direitos a ela inerentes, considerando que o tratamento das informações obtidas por essas tecnologias implica no controle e manipulação dos usuários da internet em um tempo em que a vida “real” já não pode ser isolada da digital.

E certo é que, legislar sobre a proteção de dados pessoais foi um importante avanço legislativo, contudo é necessário repensar as possibilidades regulatórias do Direito Digital na esfera da vigilância, considerando que a Lei Geral de Proteção de Dados - LGPD (Lei n.º 13.709 de 2018) e demais legislações brasileiras vigentes até o momento no âmbito digital ou informático, não cuidam da matéria, uma vez que a proteção de dados pessoais não abrange necessariamente as camadas de vigilância algorítmica, já que elas podem não atuar diretamente com os dados pessoais.

Outro fator importante a ser considerado é a aplicação de valores éticos na criação dos algoritmos, para que se possa confiar que ainda aqueles que trabalham em *machine learning*<sup>7</sup> e *deep learning*<sup>8</sup>, preservem valores que afastem vieses discriminatórios e diminuam a imprevisibilidade de suas ações.

É possível reconhecer as inovações tecnológicas como um aglomerado de prós e contras composto por um ônus robusto e opaco que implica em repercussões éticas, podendo apresentar riscos à personalidade jurídica das pessoas, se considerada a inexistência de um claro conhecimento acerca do funcionamento das tecnologias utilizadas, especialmente dos resultados daquelas que têm tomadas de decisões automatizadas por inteligência artificial.

Considera-se a inexistência de um instrumento jurídico sólido que atue preventivamente na defesa da personalidade e identidade digital dos usuários enquanto consumidores de produtos, serviços e informações, uma vez que se encontram envoltos em uma rede na qual o modelo de negócios é sustentado

---

<sup>7</sup>Aprendizagem de máquina – será abordada no tópico 4.1.

<sup>8</sup>Aprendizagem profunda de máquina – um dos desdobramentos da IA.

pela vulnerabilidade desses consumidores, que fornece dados sobre si para que sejam utilizados em seu desfavor.

Por fim, é possível concluir que a legislação apresenta um atraso frente ao exponencial desenvolvimento social e tecnológico, e considerando os moldes como a inteligência artificial tem se aprimorado, juntamente com a velocidade do seu aprimoramento, compreende-se que questões jurídicas antes impensáveis por grande parte das pessoas foram incorporadas às relações sociais atuais, sendo necessário repensar a aplicação do direito, por meio de um sistema legislativo de força preventiva, especialmente no que se refere aos métodos de vigilância que têm se aprimorado de forma autônoma e indiscriminada.

## 1.2 METODOLOGIA

A metodologia de pesquisa envolve toda a elaboração do estudo desde a definição da temática e delimitação do tema para a questão problema e objetos específicos de estudo.

A escolha do tema deve então se dar de forma que seja possível explorar melhor um assunto e para isso, o ideal é que já se tenha certo domínio da matéria, pois, um assunto totalmente “novo” demandaria uma pesquisa muito extensa de conceitos básicos e o tempo que seria empenhado em outros aspectos como na construção de uma argumentação e críticas sólidas, acaba sendo aplicado em um trabalho que ao fim não será tão robusto, (Queiroz; Feferbaum, 2019).

Quanto à robustez do texto, o importante é considerar os aspectos de um texto acadêmico de qualidade que, devem utilizar-se de uma linguagem clara, objetiva, equilibrada, expondo os estudos de forma imparcial, ainda que exista o caráter subjetivo, ele deve limitar-se às críticas construídas, mas no que se refere aos dados, há que se preservar as informações sólidas, sem distorções ou omissões. Para Queiroz e Feferbaum (2019, p. 43):

Os atributos básicos do texto acadêmico podem ser assim resumidos: (i) neutralidade e independência do autor; (ii) informação correta e completa; (iii) indicação das fontes de pesquisa; (iv) análise crítica e abrangente; (v) argumentação lógica e racional; e (vi) propostas construtivas e realistas.

Para Humberto Eco (2019), a tese, e no caso, será considerado o mesmo sentido para a dissertação, é dirigida ao orientador que por dominar o tema não precisa que sejam esclarecidos conceitos básicos, contudo, isso não afasta a necessidade de clareza e objetividade do texto, portanto, será possível e necessário fornecer ao leitor as informações mínimas para a compreensão do texto.

De início, *definem-se os termos usados*, a menos que se trate de termos consagrados e indiscutíveis pela disciplina em causa. Numa tese de lógica formal, não precisarei definir um termo como “implicação” (mas numa tese sobre a implicação estrita de Lewis, terei de definir a diferença entre implicação material e implicação estrita). Numa tese de linguística não terei de definir a noção de fonema (mas devo fazê-lo se o assunto da tese for a definição de fonema de Jakobson). Porém, nessa mesma tese de linguística, se empregar a palavra “signo”, será conveniente defini-la, pois dá-se o caso de que o termo se refere a coisas diversas em autores diversos. Portanto, teremos como regra geral: *definir todos os termos técnicos usados como categorias-chave em nosso discurso*. (Eco, 2019, p. 138).

Outro fator a ser considerado é o de que, embora exista uma hipótese ao se iniciar uma pesquisa, o pesquisador deve estar aberto às mudanças que podem ocorrer no decorrer da pesquisa, inclusive com a obtenção de resultados diferentes dos esperados inicialmente (Queiroz; Feferbaum, 2019).

No presente estudo, as hipóteses inicialmente levantadas foram de que, i) existiriam pontos cegos legislativos sobre a regulamentação dos algoritmos nas questões de vigilância e, de que ii) havendo enquadramento regulatório, haveria dificuldades de aplicação e fiscalização normativas.

Para, então, desenvolver a pesquisa, no que se refere ao critério metodológico, utilizou-se o método de análise qualitativa-exploratória. Para Queiroz e Feferbaum (2019), nesse tipo de metodologia, o pesquisador deve buscar a compreender a realidade e contextualizá-la, a partir daí ele pode fazer suas ponderações críticas analisando os pontos fracos, fortes, os possíveis riscos e as possibilidades de mitigação. Além disso, pontuações quanto a uma possível adequação legal podem compor o método exploratório.

O trabalho foi desenvolvido de forma expositiva e crítica, e considerando que a temática do Direito Digital envolve muitos aspectos que são destrinchados por diferentes autores, o estudo dispõe de uma leitura ampla, que envolveu obras

de diversos autores, mas sustenta-se, principalmente, pelas obras de Rodotà (2008) e Doneda (2019), em suas explanações sobre privacidade e proteção de dados.

## 2 INOVAÇÕES E SUAS IMPLICAÇÕES

A tecnologia teve diversos desdobramentos até que configurasse o atual modelo de vigilância, assim como os hábitos de consumo e de comunicação da sociedade, que se modificaram acompanhando essas inovações.

Para compreender o desenvolvimento desses hábitos, primeiramente é necessário saber que tecnologia e inovação são elementos distintos, e ainda que frequentemente sejam empregados como sinônimos, deve-se considerar que nem toda tecnologia caracteriza uma inovação, pois para que ocorra o processo de inovação é necessária uma incorporação social, que pode levar anos para se materializar.

Nesse sentido:

No desenvolvimento de uma tecnologia, muitas vezes, a verdadeira avaliação da importância potencial de uma invenção cabe aos outros – não necessariamente gênios tecnológicos -, que a conduzem por caminhos que o inventor jamais sonhou. O fenômeno não é nada místico: afinal, o inventor é apenas uma pessoa, com seus próprios pontos cegos, enquanto há milhões, se não bilhões, de outros olhos para enxergar novos usos que estavam bem debaixo do nariz do criador (Wu, 2012, p. 59).

Compreende-se, assim, que muitas inovações tecnológicas são criadas e se perdem sem que lhes sejam atribuídas um caráter de inovação, isso porque, “o que chamamos de invenção, embora não seja fácil, simplesmente acontece quando o desenvolvimento tecnológico chega a um ponto no qual o passo seguinte se torna acessível para muitos” (Wu, 2012, p. 27), e essa acessibilidade, quando traduzida em utilidade e aceitação pública, representa inovação.

As inovações abordadas neste trabalho trazem um entendimento necessário a respeito do trajeto de aperfeiçoamento das comunicações e fluxo de informações. O ser humano é um indivíduo comunicativo capaz de exercer tal habilidade por diversos meios. As comunicações, por sua vez, são dotadas de informações que circulam de um interlocutor a outro, e atualmente, com a internet, as linguagens de comunicação foram expandidas para diversos formatos e as informações passam a ser obtidas por meio do que se conhece por “dados digitais”.

A história das inovações percorreu invenções como telégrafo, telefones fixos, rádios, TVs, e indústria do cinema, até que se chegasse à internet, que nos seus moldes atuais é conhecida como uma tecnologia sem precedentes. As primeiras grandes inovações, no século XX, foram permeadas pelo fenômeno do “monopólio”, que controlava a economia e o mercado, tratando do acesso às tecnologias em um modelo “fechado”, não sendo acessível a todos. Dessa forma, as comunicações e circulação de informações também foram controladas pelos monopolistas.

No final da década de 1920, com todas as inovações e novidades, não apenas na área tecnológica, a sociedade começava a migrar de perfil produtivo para o perfil consumerista, mas muitos ainda não enxergavam tais modificações, e esse fluxo migratório continuou se manifestando nos anos futuros (Bauman, 2008).

As inovações supervenientes sempre “[...] deveriam ser o ápice de todas as demais [...] todas iriam mudar nossas vidas, sem dúvida, mas não a natureza de nossa existência” (Wu, 2012, p. 12).

Nessas palavras, para o autor, a internet não seria uma inovação sem precedentes, pois, observando suas antecessoras analógicas e digitais, cada inovação à sua época teria causado seus proporcionais impactos como algo nunca vivenciado antes, até que deixasse de ser novidade. As formas mais eficientes então, de se compreender o desenvolvimento das economias e das inovações, seria olhando para o passado na busca de uma interpretação sobre os possíveis desdobramentos e impactos futuros (Wu, 2012).

Magrani (2020) traz a ideia de que pela primeira vez a sociedade vivencia no presente o próprio futuro, onde o progresso é uma certeza através da revolução tecnológica, que possibilita modificações significantes nas formas de vida, interferindo nas questões econômicas e sociais. A ideia de que o momento digital vivido atualmente é sem precedentes, é corroborada por diversos autores como, Pinheiro (2021) e Bauman (2013). O que se apresenta na verdade, é que a própria tecnologia vem se superando dia a dia, em uma celeridade de fato sem precedentes.

No ramo das inovações, quando uma empresa que domina um campo da indústria ou o monopoliza, destrói as mais novas para não perder espaço no mercado, acontece o fenômeno denominado como “efeito cronos”. O termo

“cronos” deriva da mitologia Grega, quando o deus Cronos recebe de um oráculo a previsão de que um de seus filhos iriam destroná-lo. Intimidado, o deus Grego passa, então, a comer seus filhos na expectativa de manutenção do trono. Ao se considerar que as novas tecnologias surgem na busca de superação das antigas, para a indústria existente, uma nova invenção pode significar sua decadência, tornando-a de algum modo, ultrapassada (Wu, 2012).

O ciclo dos processos de inovação, narrado por Tim Wu (2012) é a alma do capitalismo, e nele quem inova prospera economicamente. Essa teoria foi inspirada no processo de “destruição criativa” de Shumpeter (2017), por avaliar que uma nova invenção supera e destrói a antiga.

O monopólio seria, então, um meio de eliminar a concorrência e consequentemente, afastar ou adiar as possibilidades de ser retirado do mercado por um produto melhor e mais inovador. As práticas de controlar o mercado podem ser mecanismos úteis frente à destruição criativa, em razão da estabilidade proporcionada para a empresa monopolista (Shumpeter, 2017).

Pensando por essa perspectiva, por muito tempo a AT&T<sup>9</sup> deixou de lançar novas tecnologias que poderiam ser concorrências para suas invenções mais rentáveis como o telefone. Um exemplo de tecnologia adiada para preservar a concorrência interna do monopólio foi a fibra ótica. Essas restrições monopolistas atrasaram em certa medida o desenvolvimento tecnológico, mas não o impediram de acontecer (Wu, 2012).

Nota-se uma supressão da democracia, e da livre escolha e iniciativa através dos monopólios, quando existe dominação do mercado por de uma única empresa, como ocorreu com a AT&T nos serviços de comunicações do século XX. Limita-se, então, as possibilidades de escolhas dos indivíduos e até mesmo o desenvolvimento de tecnologias melhores em determinada área de atuação.

A história do desenvolvimento das comunicações é importante na compreensão do consumo de produtos, serviços e informações, em razão das inovações citadas no texto terem se desenvolvido na busca pela ampliação das comunicações, o que desenvolveu e aperfeiçoou modelos informacionais, políticos e publicitários.

---

<sup>9</sup> Multinacional americana pioneira em telecomunicações, que adquiriu a Bell, sendo grande responsável pelo monopólio das comunicações em massa enquanto maior empresa de telecomunicações do mundo (Wu, 2012).

Com a então finalidade econômica, a publicidade nas rádios foi outra inovação da Bell<sup>10</sup>, isso porque a venda de aparelhos de rádio, inicialmente se apresentou lucrativa, mas não por muito tempo, uma vez que dificilmente alguma residência compraria mais de um aparelho. Já a publicidade viabilizou uma receita constante, e em 1922, a AT&T fez o primeiro anúncio comercial do rádio, contudo a utilização dos meios de comunicação para esses fins, não agradou a todos, e inicialmente houve discussões no sentido de promover uma regulamentação para que a rádio não fosse contaminada por anúncios publicitários (Wu, 2012).

A publicidade se dá através de canais de comunicação, e as informações sobre o perfil dos consumidores são primordiais para o êxito comercial. A manutenção de um fluxo informacional contínuo, como as tecnologias de vigilância, expande a viabilidade econômica, e “se a velocidade com que as informações circulam hoje cresce cada vez mais, a velocidade com que os meios pelos quais essa informação circula e evolui também é espantosa” (Pinheiro, 2021, p. 46).

Os caminhos traçados pelas inovações determinaram a rota das comunicações e das informações, que se conectam aos padrões de consumo e às formas como o mundo é recebido e percebido pelos usuários da internet.

## 2.1 AS COMUNICAÇÕES EM MASSA

As tecnologias de comunicação em massa surgem como mecanismos da economia da atenção, por se tornarem instrumentos de propagação da publicidade por meio de mídias abertas.

O desenvolvimento da rádio para uso domiciliar, por exemplo, girou em torno da publicidade por ela comercializada, o consumidor que adquirisse o aparelho de rádio, consumia a publicidade dos patrocinadores, e o mesmo aconteceu com a TV, tecnologia de inovação posterior, e hoje acontece com a internet.

[...] se olharmos com atenção o século XX, logo descobriremos que a internet não foi a primeira tecnologia da informação a

---

<sup>10</sup> Sistema Bell, Bell Company, ou Bell, fundada por Alexander Bell em 1877 (Wu, 2012).

mudar tudo para sempre. Na verdade, houve uma sucessão de mídias abertas e otimistas, mas cada qual, na devida época, tornou-se fechada e controlada por indústrias [...] (Wu, 2012, p.12).

Já era possível identificar um modelo de inovação parecido com o que foi, posteriormente, a internet. As rádios e as TVs disponibilizavam uma transmissão “gratuita”, sendo necessário apenas adquirir o equipamento. Para que os programas transmitidos pudessem se manter financeiramente, havia o “apoio” publicitário. Assim, surge o modelo de mercado por meio da atenção, e enquanto os consumidores se tornavam espectadores de programas aparentemente gratuitos, eram submetidos às propagandas comerciais, tornando-se potenciais clientes dos patrocinadores anunciados.

O molde antigo de *marketing*, que era utilizado e ainda existe nas TVs e na rádio é o de uma publicidade em massa, pensada e produzida para um público-alvo. Dessa forma, as pessoas seriam em algum momento, atraídas para o consumo. Mesmo diante de um modelo de *marketing* primário e da impossibilidade de direcionamento totalmente individualizado, o consumismo foi extremamente ampliado, surgindo uma sociedade voltada ao consumo.

A sociedade de consumidores é “o encontro de potenciais consumidores com os potenciais objetos de consumo” (Bauman, 2008, p. 19), em outras palavras, a publicidade é a promoção do encontro entre o sujeito e o objeto de desejo, que se materializa através do consumo.

Os padrões de consumo foram, então, se potencializando junto com as inovações, em outras palavras, com o surgimento de novas tecnologias e produtos, o consumidor passa a adquirir coisas que sequer sabia precisar antes que elas fossem inventadas, e as invenções e inovações, por sua vez, movimentam a indústria e o capitalismo.

As invenções podem ser classificadas em sustentáveis e disruptivas, sendo que as primeiras não promovem a queda de impérios, uma vez que atuam na melhoria dos produtos já existentes, potencializando o mercado ao invés de extingui-lo. Já as invenções disruptivas seriam as ditas destruições criativas, que superam as invenções anteriores, tornando-as inúteis e desnecessárias (Clayton M. Christensen, 2008, apud Wu, 2012).

Foi assim quando o telefone substituiu os telégrafos, e quando a TV substituiu o rádio, mas a internet é hoje a tecnologia de comunicação em massa capaz de superar todas as outras. Dentre os motivos, está o fato de que a publicidade das TVs e rádios não alcançam uma variedade comercial tão ampla como o modelo personalizado que é hoje impulsionado pela internet, onde “a cada dia o *Google* anota nossas buscas, estimulando estratégias de *marketing* customizadas” (Bauman, 2013, p. 9).

Na época em que o rádio e a TV eram as principais inovações que propagavam a publicidade, o domínio de mercado foi muito predominante, principalmente pela atuação no impedimento para que outras empresas ingressassem na mesma área de atuação, assim o conteúdo consumido e a publicidade também eram, de certa forma, controlados:

Nos anos 1940, todas as novas indústrias da informação, nos Estados Unidos e em outras partes, chegaram a uma forma estabelecida, consolidada e aparentemente duradoura, ao excluir todos os que nela pretendiam ingressar. As comunicações por rede de fios se tornaram domínio exclusivo do sistema Bell. As grandes redes, a NBC e a CBS, mandavam nas transmissões de rádio e, enquanto isso, com a ajuda da Federal Communications Commission (FCC), se preparavam para lançar sua própria imagem numa nova mídia chamada televisão. Ao mesmo tempo, os estúdios de Hollywood cerravam as cadeias em torno de todos os integrantes do setor de cinema, dos atores à distribuição (Wu, 2012. p. 18):

A prática do *truste* se refere às empresas que se fundem dominando um mercado, e detêm poder para pressionar empresas menores com o objetivo de eliminar a concorrência, (Morbidelli, 2009). Foi o que ocorreu nos Estados Unidos com o fechamento da indústria de comunicação para os que nela pretendiam ingressar. Em outras palavras, uma limitação e controle sobre quem pertenceria a esse nicho.

O fechamento para as indústrias de inovação também implicava em um controle do que chegava ao público, da publicidade aos filmes. A comunicação ocorria de forma massiva e o conteúdo era o mesmo para qualquer que fosse o espectador.

No início dos anos 1910, surgem leis para regulamentar o antitruste, buscando impedir o *truste* que na época estava ocorrendo por toda parte, desde

à indústria americana de petróleo até às rodovias. Iniciam então, investigações contra a AT&T na atuação de *truste* na área da telefonia, quando Vail<sup>11</sup> teve uma jogada política para se resguardar, fazendo um acordo com o governo e pedindo que regulamentassem as atividades de telefonia de forma justa, para que pudessem continuar a atuação na prestação de serviços (Wu, 2012).

O monopólio exercido por Vail fez com que as mídias abertas, ou seja, aquelas gratuitas aos usuários, se tornassem fechadas e de sua propriedade, acessível apenas aos clientes da AT&T. Assim, dominou fortemente o mercado das comunicações (Wu, 2012).

O Estado se mostra um importante ator no direcionamento de poderes, tendo permitido que o sistema Bell permanecesse no poder das comunicações por décadas, disfarçado de serviço de utilidade pública. Ressalta-se que a comunicação tem sim utilidade pública, mas o monopólio limitava seus avanços e sua acessibilidade, ainda assim, a empresa atuou de forma permissiva por anos.

Na década de 50, a informação era “um item caro, pouco acessível e centralizado” (Pinheiro, 2021, p. 41). Depois, com a internet, as informações se tornam mais acessíveis, nota-se que o aumento no fluxo de informação guarda relação com a expansão das comunicações.

A internet surge como um “projeto acadêmico, nada prático e altamente abstrato” (Wu, 2012, p. 193), que, se imagina, de forma desprestigiada modificou todo o direcionamento da sociedade, em termos sociais, comportamentais, econômicos e jurídicos.

Com a ampliação de acesso às comunicações de forma massiva por meio da internet, também foi expandida a dimensão da vigilância, afinal com o aumento da comunicação, a quantidade de informações em circulação cresceu exponencialmente.

A sociedade da informação vivencia os excessos em seu sentido mais amplo, quando a hiperconexão mantém a um clique o objeto de desejo, desde informações até o consumo de praticamente tudo o que se possa imaginar. Esse modelo é sustentado por bases de dados constantemente alimentadas pelos dados de navegação, e que formam o *Big Data* - conjunto de dados

---

<sup>11</sup> Theodore Vail, presidente da AT&T (Wu, 2012).

armazenados -, possível pela utilização excessiva da internet e tecnologias inteligentes.

## 2.2 INFORMÁTICA E INTERNET

O processo de inovação é constante, as tecnologias vão se aprimorando ou por uma demanda populacional, ou criam uma demanda a partir de suas funcionalidades. Foi o caso da informática em que suas funcionalidades criaram novas atividades a serem atendidas por essa tecnologia.

Patrícia Peck Pinheiro (2021) definiu a informática como uma tecnologia capaz de realizar diversas funções, melhorando outras já existentes, ou criando novas metodologias por meio da automatização de atividades, através de um sistema de tratamento de dados e informações, que é o computador. É uma facilitadora de processos manuais repetitivos, automatizando-os e trazendo agilidade para as mais diversas rotinas, que trabalham com armazenamento e processamento de informações, desde cálculos até os mais diversos bancos de dados.

A informática surge a partir de experiências matemáticas, que buscaram facilitar cálculos, tendo sido realizados diversos projetos por diferentes especialistas da área, até que em 1951, o UNIVAC I, surge como o primeiro computador comercial (Pinheiro, 2021).

Na década de 60, os computadores, ou seja, a informática existente, não guardava relação com a mobilidade atual, as máquinas restritas à propriedade de empresas e dos governos, eram utilizadas para processamento de dados, sendo gigantescas, ocupando uma sala inteira, (Wu, 2012).

Com todo o processo de informatização, ideias surgiram em torno das possibilidades de tornar as máquinas mais funcionais e aproximá-las dos homens comuns. Engelbart<sup>12</sup> e Licklider<sup>13</sup> foram dois dos idealizadores desse conceito, “mas nenhum dos dois estava perto de definir como se poderiam combinar na prática as capacidades humanas e as dos computadores”, (Wu,

---

<sup>12</sup> Douglas Carl Engelbart, engenheiro e um dos pioneiros das invenções da computação e internet.

<sup>13</sup> Joseph Carl Robnett Licklider, cientista da computação também pioneiro nas invenções da época.

2012, p. 209). Embora, à época, as invenções de Engelbart estivessem distantes do que hoje se conhece por computador, foi ele o inventor responsável por introduzir *hardwares* básicos, ainda utilizados, como o teclado e o mouse (Wu, 2012).

Ao longo do desenvolvimento informático, destacam-se alguns feitos:

O primeiro computador com *mouse* e interface gráfica é lançado pela Xerox, em 1981; já no ano seguinte, a Intel produz o primeiro computador pessoal 286. Tim Bernes Lee, físico inglês, inventa a linguagem HTML (*Hyper Text Markup Language*, em português, Linguagem de Marcação de Hipertexto), criando seu pequeno projeto de World Wide Web (WWW), em 1989; Marc Andreessen cria o *Browser Mosaic*, que permite fácil navegação na Internet, em 1993. Em 1996, Steve Jobs lança o iMac. No mesmo ano, dois estudantes americanos, Larry Page e Sergey Brin em um projeto de doutorado da Universidade Stanford, criam o maior *site* de buscas da internet, o “Google” (Pinheiro, 2021, p. 55).

A informática se associa à internet, tornando-se com o tempo, um veículo de comunicação que fez surgir o “ambiente digital”, que hoje está mais associado à internet, pois, a informática e a internet que são, em verdade, dois elementos distintos, hoje parecem uníssonas (Pinheiro, 2021).

O formato atual da internet só foi possível com a expansão da informática para além de máquinas de cálculos, contudo, internet e informática são conceitos que se confundem em razão de uma não poder ser a inovação que é, sem que estivesse atrelada à outra (Wu, 2012).

Para Bernardi (2020, p. 21) “[...] assim como o rádio revolucionou o jornal impresso e a televisão revolucionou o rádio, podemos dizer que estamos vivendo uma revolução digital, na qual a internet é o combustor da era da informação”.

A internet opera por meio da informática, e sua popularidade está vinculada à informatização cada vez mais presente nas atividades cotidianas.

[...] a Internet veio possibilitar não apenas o encurtamento das distâncias com maior eficiência de custos, mas, sobretudo, a multicomunicação, ou seja, transmissão de texto, voz e imagem. A multicomunicação, associada à capacidade de respostas cada vez mais ágeis, permite que a Internet se torne o mais novo veículo de comunicação a desafiar e transformar o modo como nos relacionamos. (Pinheiro, 2021, p.56).

A internet, enquanto tecnologia sem precedentes, é analisada a partir do ponto de vista onde se reconhece que o telefone foi a primeira grande ferramenta que viabilizou a comunicação de forma simultânea, interferindo e influenciando nos comportamentos sociais da época, contudo a internet superou o telefone, o rádio e a TV, pois, além de ser uma ferramenta de multicomunicação, por transmitir imagem, texto e voz, ela permite que se tenha respostas instantâneas. Esse modelo superou qualquer outro meio de comunicação já existente (Pinheiro, 2021, p. 56).

Apesar da simplicidade dos termos, o surgimento e popularização da internet não foi um processo fácil, e retoma as questões do controle de mercado. Nos anos 60, quem monopolizava as comunicações e redes, era a AT&T, a empresa de telefonia era detentora das comunicações de longa distância e introduzir a tecnologia da internet estaria vinculada ao seu sistema de comunicações. Licklider foi o primeiro na época a identificar a rivalidade existente entre telefonia e computação, uma vez que acreditava que a computação proporcionaria, futuramente, uma comunicação mais eficiente até mesmo que a física (Wu, 2012).

Diversas histórias e invenções tecnológicas se cruzaram até que a internet chegasse ao que é conhecida hoje, e no percurso da inovação a FCC<sup>14</sup> proibiu que a AT&T participasse de forma direta do então mercado de processamento de dados e serviços on-line, (Wu, 2012).

Em resumo, com uma visão de futuro estranha e sem precedentes, a FCC regou, adubou e cultivou os serviços on-line para computadores como uma indústria especial e protegida, estabelecendo ao longo dos anos uma série de regras chamadas de "Computer Inquiries", um regime complexo construído para evitar que a AT&T destruísse qualquer empresa nascente e garantir que os serviços on-line para computadores se desenvolvessem sem regulamentação. Importante para o destino das telecomunicações e para nossa narrativa é que a indústria nascente, protegida pela FCC nos anos 1970, se transformou em companhias como America Online, CompuServe e outras empresas de redes on-line (os provedores de serviços de internet). (Wu, 2012, p.231).

---

<sup>14</sup> Federation Communications Commission é a agência do governo dos Estados Unidos que regula as comunicações.

Na contramão de toda essa evolução, havia a AT&T tentando manter seu monopólio, e prejudicando as empresas que se aventuravam pela área da comunicação. A questão envolta trata de poder e controle, quem detém o acesso à comunicação detém o controle sobre as informações e toda essa demanda por poder atrasou o desenvolvimento e chegada das redes de internet à população comum.

Na década de 70, ainda não existia essa conexão universal idealizada, mas os computadores de universidades e do governo americano podiam se comunicar por meio da *ARPAnet*<sup>15</sup> que utilizava linhas telefônicas da AT&T para conexão. Na mesma época, havia outras duas redes de internet em desenvolvimento, sendo que, uma utilizava o sistema de conexão por rádio e a outra por satélite, (Wu, 2012).

A *ARPAnet* era um sistema descentralizado de comunicação informático que permitia a comunicação entre computadores militares, preservando sua segurança em razão de não dispor de uma central única de informações. Um tempo depois, as universidades americanas ganharam acesso ao sistema para fins acadêmicos, e a partir do ingresso da internet na academia, com o menor controle do sistema, houve a possibilidade de aperfeiçoamento e melhor desenvolvimento da rede (Pinheiro, 2021).

Para se tornar um meio de comunicação ilimitado, a internet precisaria aplicar uma linguagem comum – linguagem única - entre as redes, para que fosse possível, por exemplo, que uma rede acessada por meio de uma linha discada se comunicasse com redes de internet a rádio ou via satélite, e esse foi outro processo a ser desenvolvido para universalização da internet, uma linguagem única de computadores.

Com essa finalidade, foi implementado o *Transmission Control Protocol* (TCP<sup>16</sup>) que, possibilitou aos usuários da internet, a utilização de uma linguagem entendível a qualquer tipo de rede, era “uma rede eletrônica de informação independente da estrutura física na qual funcionava”, (Wu, 2012, p. 240).

---

<sup>15</sup>Rede de Agências de Projetos de Pesquisa Avançada, de 1969, rede experimental, projetada para transmitir dados sigilosos militares e conectar departamentos de pesquisas dos EUA (Snowden, 2019).

<sup>16</sup>Protocolo de Controle de Transmissão é um dos protocolos de comunicação, da camada de transporte da rede de computadores (Pinheiro, 2021).

Em outras palavras, a internet implantou uma realidade de comunicação universal, por meio de um sistema autônomo e descentralizado. A comunicação é universal e não o sistema, pois, as formas e redes de acesso são variadas, embora possam se comunicar:

[...] a internet é, na verdade, uma “rede de redes”. Isso significa que a internet é um conjunto de redes particulares, interconectadas a partir de um mesmo protocolo (o TCP/IP) e seguindo os mesmos padrões técnicos de interoperabilidade, o que permite a comunicação entre diferentes localidades (Ramos, 2018, p. 87).

No final da década de 80, a utilização da internet passou aos fins comerciais, sofrendo exponencial crescimento na década de 90, com novos recursos, melhor acessibilidade aos usuários, popularização na utilização de *e-mails* (correio eletrônico), conectando usuários do mundo inteiro por meio de linhas telefônicas, fibra ótica, satélite, ondas de rádio ou infravermelho (Pinheiro, 2021).

Os movimentos da tecnologia avançaram e continuaram se aprimorando. A internet de hoje – 2023 – não é a mesma da década de 90, assim como a informática também ficou mais tecnológica. Hoje, a internet está por toda parte, a comunicação ocorre a todo momento, assim como a coleta e tratamento de dados. Isso acontece em razão dos usuários da internet disporem de uma conexão *mobile*<sup>17</sup> e *smart*, que os acompanham por toda parte, por meio de tecnologias persuasivas de vigilância que podem, inclusive, se comunicar entre si, coletando dados com finalidade comercial.

## 2.3 O “NOVO” CONSUMIDOR

Toda a dinâmica da inovação e desenvolvimento tecnológico influenciaram na formação de perfil dos novos consumidores, tanto em relação ao consumo de serviços e produtos, como no que se refere ao consumo informacional, quando o consumidor, por exemplo, se encontra na posição de

---

<sup>17</sup> Tecnologias que permitem mobilidade, como os *smartphones*.

eleitor, ou na própria estruturação de suas ideologias pessoais e construções de ideias.

Os sistemas primários de comunicação tecnológica, como a rádio e a TV, se deslocaram de um papel informacional centralizado para um modelo em que as pessoas têm a possibilidade de escolher para onde direcionar sua atenção. Com o acesso à diversidade de fontes de informações, o consumidor enquanto espectador, se torna mais seletivo, podendo escolher qual conteúdo pretende consumir. Em outra esfera, o consumidor também adquire a possibilidade de produzir conteúdo e todos se tornam parte de uma geração de “especialistas em tudo”, onde se pode ser produtor e consumidor (Florêncio, 2019).

A partir da democracia do espaço virtual, torna-se necessário uma atenção aos conteúdos que são consumidos, uma vez que qualquer pessoa pode produzi-los, tornando as fontes sensíveis em sua veracidade, como acontece com as *fake news*<sup>18</sup> e qualquer outro conteúdo de caráter desinformativo com capacidade para influenciar.

As influências nos padrões de consumo se desenvolveram através da publicidade e das próprias inovações que incorporavam o desejo pelas novas invenções e suas facilidades. Atualmente, o direcionamento da vontade em adquirir algo ou do interesse em dedicar atenção a determinado tipo de informação está relacionado à vigilância algorítmica e suas possibilidades de persuasão.

É importante considerar que muitos consumidores estão satisfeitos com o modelo de *marketing* digital por ser capaz de lhes oferecer algo que guarde relação com seus desejos e preferências, como quando a *Amazon*<sup>19</sup> sugere um livro baseado nas compras anteriores ou na lista de desejos de determinado usuário. Isso parece ótimo por encurtar o trabalho que o consumidor teria em passar horas escolhendo um livro, contudo é na verdade uma “bolha de filtro” (Bauman; Lyon, 2013).

Essa ideia de “bolha de filtro” diz respeito ao direcionamento dado na filtragem das pesquisas, conduzindo os resultados a temas que interessem aos usuários, contudo limitando seus horizontes uma vez que estarão condenados

---

<sup>18</sup>Será conceituada no capítulo 5.

<sup>19</sup>Empresa multinacional de tecnologia norte-americana. Uma das gigantes da tecnologia na sociedade atual.

às próprias ideias e percepções, mantendo, por exemplo, sempre o mesmo nicho de leitura (Bauman; Lyon, 2013).

Outra característica negativa deste modelo de filtro, é a supressão de produtos e marcas que perdem espaço para se tornar conhecidas, mantendo em alta os mesmos autores, empresas e produtos.

A ubiquidade da internet faz com que o consumo tenha a mesma característica, e as tecnologias de persuasão se aproveitam dessa onipresença digital para oportunizar o consumo a todo momento por meio da “publicidade comportamental”. As tecnologias percebem o melhor momento para oferecer determinado anúncio a consumidor, pois através dos dados pessoais é possível identificar e rastrear padrões de consumo, comportamentos e preferências políticas (Florêncio, 2019), além das vulnerabilidades, como que tipo de informação deixa o usuário triste ou feliz.

A internet enquanto veículo de comunicação em massa, se mostra como um ambiente digital repleto de serviços “gratuitos”. O que na verdade é um modelo de negócios denominado por, *zero-price advertisement business model*<sup>20</sup>, que disponibiliza serviços aparentemente gratuitos e remete à expressão: “quando você não paga para utilizar determinado produto, o produto é você”. Isso em razão dos usuários “aceitarem” utilizar os serviços em troca da disponibilização de seus dados pessoais, o que ocorre nas plataformas do *Waze*<sup>21</sup> e do *spotify*<sup>22</sup>, por exemplo (Sanches; Curiati, 2019), nas quais o acesso deixa rastros digitais de seus usuários.

Os rastros digitais dos consumidores podem se dar da seguinte forma:

A sequência de cliques (*clickstream*), também denominado rastro de cliques compõe o registro da trajetória que um usuário percorre ao clicar em determinado local em página da internet. Esses dados são capturados por tecnologias como *cookies* e passam a ser analisados com vista a entregar resultado informativo – muitas vezes por meio de venda (*data broker*) – para pesquisas de mercado, produtividade de empregados e, especialmente, para publicidade comportamental (Florêncio, 2019, p. 53).

---

<sup>20</sup>Modelo de negócios de publicidade com preço zero (Sanches; Curiati, 2019).

<sup>21</sup>Waze é uma aplicação para dispositivos móveis, baseada na navegação por GPS (Sanches; Curiati, 2019).

<sup>22</sup>Spotify é um serviço de streaming de música, podcast e vídeo (Sanches; Curiati, 2019).

Os usuários disponibilizam suas informações enquanto navegam para, em troca, utilizarem serviços, como se trocassem privacidade por acessibilidade:

A troca de metadados por serviços de comunicação tornou-se a norma; poucas pessoas parecem dispostas a pagar por mais privacidade. Seu uso como moeda para pagar pelos serviços on-line e por segurança tornou os metadados uma espécie de ativo invisível, processados, na maioria das vezes, fora de seu contexto original e sem que as pessoas tenham consciência. As companhias de mídia social monetizam os metadados ao reprocessá-los e vendê-los para anunciantes ou companhias de dados (Dijck, 2017, p. 45).

O estudo de perfil do consumidor atual, acontece em tempo real e é possibilitado pelos próprios hábitos de consumo desse indivíduo, quando “identificar padrões de conduta ou de atividades inconscientemente deixadas nos (meta)dados dos sites de redes sociais cada vez mais serve para prever o futuro” (Dijck, 2017, p. 43).

O espaço digital é amplo e multitemático, contemplando interesses obscuros por trás de serviços aparentemente gratuitos, jogos, e até mesmo nos objetos inteligentes que são levados para dentro da casa do usuário, ou acoplados ao seu corpo (*wearables*<sup>23</sup>).

Cientistas de dados explicam que o interesse das plataformas não está nas atividades executadas pelos usuários ou no que elas estão fazendo no momento presente. A valoração dos dados está mais associada a possibilidade de prever comportamentos futuros (Weerkamp; Rijke, 2012, apud Dijck, 2017).

O perfil do consumidor é mutável, seja na aquisição de produtos ou na formação de uma opinião política, é possível moldar o comportamento desse indivíduo, e a condição de insatisfação permite a flexibilidade para recepção de novas informações.

A vida do consumidor, a vida de consumo, não se refere à aquisição e posse. Tampouco tem a ver com se livrar do que foi adquirido anteontem e exibido com orgulho no dia seguinte. Refere-se, em vez disso, principalmente e acima de tudo, a *estar em movimento*” (Bauman, 2008, p. 126).

---

<sup>23</sup>As tecnologias vestíveis ou dispositivos vestíveis, são tecnologias que se apresentam na forma de dispositivos iguais ou similares a peças de roupa ou equipamentos vestíveis, tais como relógios, pulseiras ou até mesmo óculos de realidade virtual (Magrani, 2019).

Apesar de toda a aparente complexidade comportamental, conhecer o perfil de um consumidor ou eleitor e persuadi-lo a mudar, nunca foi tão acessível para as empresas como é hoje. Os riscos do consumo digital e informacional vão além da aquisição de bens e serviços, implicando em questões democráticas que serão abordadas junto às temáticas de política e desinformação.

### 3 DATIFICAÇÃO DA PERSONALIDADE

As modificações sociais e tecnológicas que impactaram no consumo são próprias do excesso de dados pessoais fornecidos pelas pessoas hiperconectadas. O estado da sociedade de hoje é totalmente informacional, e a informação nunca foi tão importante antes.

As pessoas estão se tornando *networked persons*, em outras palavras, pessoas conectadas à rede de forma contínua, possibilitando uma interferência externa na autonomia pessoal (Rodotà, 2008).

As redes sociais foram grandes responsáveis pelo interesse dos usuários da internet em migrarem suas relações sociais para o ambiente virtual. Permanecendo conectados por mais tempo, os indivíduos tiveram a codificação de muitas esferas de sua vida social, como inter-relações, conhecimento de interesses através de pesquisas realizadas nos motores de buscas, respostas emocionais, conversas casuais, e conteúdo acessado diariamente (Dijck, 2017).

As empresas de tecnologia, visualizando as possibilidades econômicas, se especializaram nas comunicações e interações virtuais, com isso a “transformação digital da sociabilidade produziu uma indústria na qual seus progressos estão baseados no valor dos metadados” (Dijck, 2017, p. 42).

As relações jurídicas existentes são permeadas pelo fornecimento de dados decorrentes de informações coletadas por meio do preenchimento de fichas para cadastros, respostas às pesquisas, fornecimento de CPF<sup>24</sup> no momento de uma compra, dentre outros meios utilizados para captar dados pessoais.

Todos esses processos raramente são questionados pelo consumidor que frequentemente fornece seus dados sem ter o conhecimento da finalidade. Talvez falte tempo para questionamentos, ou reflexão sobre o fato de que os dados coletados formarão o perfil desse indivíduo enquanto consumidor e “serão acessados, vendidos, comprados e usados pelas empresas em suas estratégias de *marketing*” (Sibila, 2015, apud Florêncio, 2019, p. 52).

O usuário das tecnologias de vigilância se configura como produto dos seus objetos (suas coisas conectadas), sendo que a sua vida se torna fonte de

---

<sup>24</sup> Cadastro de pessoas físicas.

alimentação de um sistema que utilizará das informações fornecidas contra ele próprio.

As informações sobre o perfil dos usuários “podem ser usadas para aperfeiçoar serviços de plataforma personalizados e oferecer aos psicólogos sociais uma riqueza de dados que eles nunca poderiam obter de outra forma” (Dijck, 2017, p. 44).

A atenção é voltada para o entrelace entre tecnologia, inovação, consumo e perfil, ou público-alvo. Toda a arquitetura das tecnologias atuais parece estar voltada para uma finalidade econômica, possibilitada pelo entendimento de padrões dos usuários da internet, e o fornecimento de dados por meio do excesso de conectividade, permite um maior conhecimento.

Os fatores narrados levam a datificação da personalidade, conceito implementado por Mayer-Schoenberger e Cukier (2013, apud Dijck, 2017, p. 41) como:

[...] a transformação da ação social em dados on-line quantificados, permitindo assim monitoramento em tempo real e análise preditiva. As empresas e as agências governamentais exploram as pilhas exponencialmente crescentes de metadados coletados a partir da mídia social e plataformas de comunicação, tais como *Facebook*, *Twitter*, *LinkedIn*, *Tumblr*, *iTunes*, *Skype*, *YouTube*, e serviços gratuitos de e-mail, como o *Gmail* e o *Hotmail*, para rastrear informações sobre o comportamento humano [...] A datificação, como um legítimo meio para acessar, entender e monitorar o comportamento das pessoas está se tornando um princípio central, não apenas entre os adeptos da tecnologia, mas também entre os acadêmicos que a veem como uma revolucionária oportunidade de pesquisa para investigar o comportamento humano.

Em outras palavras, todos os dados utilizados para alimentar bancos de dados, a partir do processamento por algoritmos que os transformam em “conhecimento”, moldam uma personalidade digital do indivíduo, transformando o “eu” em dados, uma espécie de figura digital de representação da vida real, a “datificação da personalidade”.

Essa representação - datificação - possibilita, então, que empresas e agências governamentais tenham uma previsão de comportamentos futuros através da análise preditiva, um processo que:

[...] usa análise de dados, machine learning, inteligência artificial e modelos estatísticos para encontrar padrões que possam prever comportamentos futuros. As organizações podem usar dados históricos e atuais para prever tendências e comportamentos com segundos, dias ou anos de antecedência, com muita precisão. [...] Os cientistas de dados usam modelos de previsão para identificar correlações entre diferentes elementos nos conjuntos de dados selecionados. Quando a coleta de dados é concluída, um modelo estatístico é formulado, treinado e modificado para gerar previsões precisas (Google Cloud, [20--?]).

Nesse sentido, se pelo prisma econômico a datificação da personalidade traz inúmeros benefícios como a possibilidade de utilizar técnicas de análises preditivas para: 1. Detectar fraudes. 2. Prever estratégias para converter ações de marketing em compras; 3. Reduzir riscos financeiros; 4. Melhorias internas de gestão; 5. Classificação de clientes, etc (Google Cloud, [20--?]), por outro ângulo pode implicar em riscos à personalidade e à privacidade do indivíduo.

### 3.1 INTERNET MÓVEL E MÍDIAS SOCIAIS

A sociedade da informação é uma geração que vivencia um tempo diferente, onde as informações estão acessíveis a todo momento e a tecnologia se desenvolve suprimindo algumas necessidades e criando outras.

Na década de 90, os *paggers* ou bipes eram dispositivos utilizados para comunicação por meio de transmissão via rádio, mas necessitavam de uma interlocução via central de atendimento que teria de ser acionada através de ligação telefônica, na época, realizada a partir de um telefone fixo, solicitando que a central transmitisse determinada mensagem de texto. Esse tipo de equipamento era receptivo, não enviava mensagens, apenas as recebia (Coelho, 2018).

Posteriormente, surgem no Brasil, os telefones móveis analógicos, que dispunham de baixa tecnologia, sendo possível realizar interceptação das ligações telefônicas com pouco conhecimento técnico. A segunda geração de telefones móveis era um pouco mais segura e, no Brasil de 2002, trazia a possibilidade de conexão à internet, vindo a se popularizar anos depois, com a melhora nas tecnologias dos aparelhos e, também, na qualidade de navegação (Figueiredo, 2023).

A internet móvel acompanha o sujeito de dados em toda parte, com a acessibilidade na palma das mãos, como explica Pinheiro (2021, p. 448 – 449):

A Internet móvel vem atender às necessidades do surgimento de uma sociedade com iguais características, em que os indivíduos se deslocam o tempo todo e carregam a possibilidade de ser identificados e localizados eletronicamente a qualquer momento.

A Sociedade Digital Móvel traz acessibilidade vinte e quatro horas por dia aos seus membros, mesmo quando em deslocamento. Essa funcionalidade pode ser vantajosa, mas ao mesmo tempo é um pouco aflitivo pensar que “alguém” pode saber por onde você andou durante todo o tempo e o que fez. Mais uma vez, estamos diante de uma situação de confronto entre segurança e privacidade.

Esse conflito entre segurança e privacidade, diz respeito ao ônus que recai sobre os usuários, em razão da utilização e exposição às tecnologias invasivas, presentes na sociedade da informação, e a perda da privacidade e alimentação constante de bancos de dados. O que inicialmente pareceu liberdade, agora gera uma preocupação com a proteção do indivíduo, que se encontra a todo tempo monitorado, uma vez que vive cercado por tecnologias inteligentes.

A tecnologia dos telefones móveis se desenvolveu através de uma diversidade de modelos de *smartphones*, e a popularização da internet móvel para as massas se deu, especialmente, em razão da expansão das redes sociais. Além disso, depois de algum tempo, todos os aparelhos de telefone passaram a ser desenvolvidos com tecnologias modernas, como *touchscreen* (tela sensível ao toque), superando modelos primários e com poucos recursos.

As redes sociais são perfis criados pelos usuários da internet, onde eles podem configurar suas contas como públicas ou privadas e compartilhar mídias com amigos e desconhecidos – fotos, vídeos, áudios – de suas experiências pessoais ou posicionamentos sobre determinado assunto. Podem criar um espaço social virtual e interagir com outras pessoas, e os interesses desses indivíduos em participar dessas interações sociais como expositores ou espectadores, ampliaram e ampliam o uso da internet (Zampier, 2021).

A partir do entretenimento das redes sociais, a internet ganha espaço e sua utilização se propaga até se tornar um meio massivo de comunicação,

despertando interesses econômicos a partir das possibilidades vislumbradas no excesso de sua utilização, o que permitiu uma identificação mais precisa do perfil dos usuários, despertando interesses comerciais.

Ao passo que mais aplicativos eram desenvolvidos, a constância na utilização do aparelho de celular inteligente, também aumentava, se tornando necessário e útil. A partir dessa digitalização das funções cotidianas, também surge a digitalização das relações interpessoais por meio das redes sociais. Gradualmente, os usuários da tecnologia ingressam no ambiente virtual de forma que, atualmente, tornou-se difícil separar vida digital e real.

Em uma crítica às redes sociais e monitoramento, Lanier (2018, p. 13) explica que:

Nos últimos cinco ou dez anos, quase todo mundo começou a carregar consigo, o tempo todo, um aparelhinho chamado *smartphone*, feito sob medida para modificações de comportamento pelos algoritmos. Muitos de nós também usam aparelhos chamados *smart speakers* (alto-falantes inteligentes) na bancada da cozinha de casa ou no painel do carro. Estamos sendo rastreados e avaliados constantemente, e recebendo o tempo todo um *feedback* artificial (Lanier, 2018, p. 13).

O autor expõe sua preocupação de que as mídias sociais e o excesso de tecnologias a que as pessoas são expostas, as submetem a um constante monitoramento, no qual a finalidade dirigida a esse fluxo de dados é obscura, sendo as tecnologias *smarts* e as redes sociais protagonistas na coleta e tratamento de dados.

A primeira rede social, no formato de compartilhamento de mídias e de exposição virtual, que ficou popular no Brasil, foi o extinto *Orkut* (2004), desenvolvido pelo *Google Inc.*, em seguida o *Facebook*, uma rede criada por estudantes universitários, se consolidou como a maior rede social, levando o *Orkut* à extinção (Zampier, 2021).

O *Facebook* se tornou uma das mais importantes redes sociais no que se refere à coleta e tratamento de dados de forma obscura. A empresa Meta Inc. que hoje comanda, além do *Facebook*, o *Instagram*, o *Messenger* e, também, o *WhatsApp*, já se envolveu em diversos escândalos sobre vazamento de dados pessoais de seus usuários.

A sociedade hiperconectada ou da informação se representa como a sociedade do espetáculo, por meio de comportamentos de exposição constante e imersão nas redes sociais, demanda sempre uma necessidade de ser vista de um ângulo que lhe proporcione o “parecer melhor” do que de fato é, o indivíduo que vive no espetáculo aliena a si mesmo em prol da construção de uma imagem exibida nas redes sociais (Zampier, 2021).

A mobilidade digital por meio dos dispositivos inteligentes, potencializa a sociedade do espetáculo, uma vez que as pessoas carregam objetos de monitoramento por toda parte, objetos que se tornam “desejo” de consumo de muitas pessoas em razão da representação social que podem ter. O tempo disposto para as redes sociais revela muito sobre comportamento, preferências e interesses.

Trata-se então, de uma sociedade extremamente conectada, que a partir dos mais diversos meios, alimenta bancos de dados a todo momento, isso considerando, por exemplo, as tecnologias de monitoramento do sono presentes em aparelhos domésticos e acessórios, como os *smart watches* (relógios com tecnologia inteligente), que não descansam enquanto seus usuários dormem.

Estamos vivendo a cultura das interfaces gráficas, conforme muitos autores já descreveram, em que o computador, de fato, transforma nossa maneira de criar e comunicar na era digital. Não apenas apelidos avatás, mas verdadeiras redes sociais estão sendo construídas, onde as pessoas se relacionam completamente de modo eletrônico, trabalham juntas, namoram, sem nunca se terem encontrado pessoalmente. (Pinheiro, 2021, p. 457).

O excesso de digitalização da vida e a exposição às redes sociais, levantam problemáticas sobre privacidade, proteção de dados, e o limite entre liberdade de expressão e o direito de terceiros. Além disso, já foi possível identificar como o direcionamento de conteúdo por meio de algoritmos, nas redes sociais, influencia na polarização de ideias, preferências comerciais e políticas (Pinheiro, 2021).

A conectividade está por toda parte e não há como fugir dessa realidade virtual, mas é necessário que o Direito também acompanhe tais incorporações digitais nas movimentações sociais, e esteja preparado para regulamentar modelos de relações nunca antes vislumbrados.

### 3.2 TECNOLOGIAS DE VIGILÂNCIA

A conectividade onipresente é representada pela comunicação entre objetos – coisas – e seus usuários. Com a expansão do mercado tecnológico e diversas possibilidades de aparelhos e objetos inteligentes, associados aos padrões de consumismo excessivo, os usuários da internet fornecem dados sobre si mesmos de forma contínua.

O modelo de conexão permanente pode ser chamado de *hiperconectividade* e extrapola a ideia de conexão para comunicação constante. Compreende-se a hiperconectividade a partir de alguns desdobramentos, 1. *Always-on*, pessoas que ficam conectadas o tempo todo; 2. *Readily accessible*, o estado em que a pessoa está prontamente acessível; 3. *Always recording*, o fluxo constante de informações e o armazenamento contínuo de dados. A hiperconectividade pode ser entendida como a comunicação não apenas entre indivíduos, mas também indivíduo-máquina e até mesmo a comunicação entre as máquinas, sendo que em qualquer dos contextos, predomina um grande fluxo de dados (Magrani, 2019).

A datificação da personalidade surge quando se coloca no digital as características e elementos da vida de uma pessoa. E essas possibilidades de inserir no ambiente virtual os dados de uma vida *off-line*, ocorrem por meio dos dispositivos inteligentes e do excesso de conectividade. Com a datificação, os seres humanos adquirem uma projeção do seu “eu” no ambiente digital, no formato de uma personalidade e imagem pessoal digitais (Rodotà, 2008).

O fenômeno de se conectar com objetos - coisas - inteligentes foi denominado por IoT, (do inglês, *Internet of Things*). A internet das coisas diz respeito a dispositivos eletrônicos e digitais incorporados à rotina das pessoas e que são capazes de, por meio de sensores, captar dados e utilizá-los de formas inteligentes. Os dados captados pelas tecnologias inteligentes presentes nesses dispositivos são os mais variados, desde vozes, à presença, temperatura, localização, mapeamento de ambientes, movimentação, humor, etc (Magrani, 2019).

A aplicação da IoT pode ser resumida, nas palavras de Magrani (2020, p. 20), como um “ambiente de objetos físicos interconectados com a internet por

meio de sensores pequenos e embutidos, criando um ecossistema de computação onipresente (ubíqua), voltado para a facilitação do cotidiano”.

O estado de hiperconexão dos usuários da internet gera um imenso volume de dados com formatos diferentes, decorrentes dos rastros de conexão, deixados pelos usuários e unindo os conceitos de IoT e *Big Data*, enquanto as tecnologias de vigilância alimentam esse grande banco de dados. Os problemas surgem quando a reflexão se movimenta da esfera do conforto do consumidor com seus dispositivos inteligentes, para as relações jurídicas decorrentes da coleta, processamento e compartilhamento de dados particulares e íntimos, interferindo na esfera da privacidade e segurança pessoal dos indivíduos (Magrani, 2020).

A datificação da personalidade reflete um conhecimento profundo dos indivíduos enquanto usuários da internet, possibilitando que sejam segmentados em perfis individuais, ou em grupos, de forma que o conteúdo seja assertivamente direcionado, atingindo o sujeito a quem possa interessar. Esse direcionamento é uma forma de controle informacional que pode impactar as democracias, contudo mascarado pelo acesso indiscriminado dos usuários aos conteúdos *on-line*.

A extensão do conhecimento que as gigantes da tecnologia têm sobre seus usuários, leva às possibilidades de persuasão comportamental. O termo tecnologia persuasiva foi introduzido por Fogg e “é definida como uma tecnologia desenvolvida para mudar atitudes ou comportamento dos usuários através de persuasão e influência social, sem o uso, porém, da coerção”, (Nascimento, *et al.*, 2018, p. 3).

Com um perfil bem delineado por meio da excessiva coleta de dados, a persuasão será sempre mais satisfatória, sendo assim, aqueles que passam mais tempo conectados encontram-se mais vulneráveis. O ambiente digital, é um território de monitoramento constante, pouco percebido pela maior parte dos usuários, mas muito explorado como recurso, pelos aplicadores do *marketing* digital. Isso porque a potencialidade das redes e plataformas sociais e digitais, ignorada por muitos, é sustentada por fatores econômicos e comerciais.

A digitalização da vida social com as interações e relações interpessoais se dando, a quase todo tempo, por intermédio das plataformas digitais e tecnologias como as presentes na internet das coisas, permite que as empresas

do ramo da vigilância conheçam afundo o perfil de seus usuários, podendo comercializá-los para outras, para que sejam explorados com finalidades comerciais ou, até mesmo, políticas.

Com tecnologias *smart* (inteligentes) sempre por perto e conectadas à internet, seja por meio do *smartphone*, *smart tvs*, *smartwatch's*, etc., a inteligência permeia as relações humanas coletando os mais variados dados: desempenho na corrida; horas de sono por noite; plataforma de *streaming* mais utilizada, etc. E como o próprio nome sugere, *smart*, os aparelhos e acessórios inteligentes também funcionam por meio da tecnologia de inteligência artificial.

A ideia de vigilância que antes era decorrente dos rastros deixados pelos usuários quando utilizavam o ambiente *on-line*, agora pode ser, também, incorporada “para o mundo físico por meio das coisas e objetos presentes no cotidiano do ser humano. Ela se torna mais intrusiva e opaca” (Bioni, 2021, p. 87).

As relações humanas foram modificadas pela hiperconectividade, e a possibilidade de a comunicação ir além de seres humanos e máquinas, compondo também relações não humanas, como aquelas entre dispositivos conectados e máquinas, demonstrando que a esfera pessoal do indivíduo pode ter interferências algorítmicas em razão dos desdobramentos do fluxo de informações automatizadas, o que requer uma análise ética sobre a cultura e opacidade algorítmica.

## 4 VIGILÂNCIA ALGORÍTMICA

A crescente integração da tecnologia à realidade humana, seja pela permanência das pessoas nos ambientes digitais, seja por meio da incorporação do virtual à esfera física, trouxe vantagens e em contraposto, desafios complexos como a vigilância algorítmica, que implica interferências do digital nas esferas da privacidade e democracia.

O fenômeno da vigilância algorítmica opera por meio de algoritmos de inteligência artificial no processo de coleta, análise, e interpretação de dados pessoais dos usuários da internet e tecnologias digitais. Trata-se de uma visão ampla da vida digital que alimenta bancos de dados constantemente, possibilitando traçar perfil de indivíduos e prever seus comportamentos futuros, o que implica nas questões de privacidade.

O ambiente digital é um cenário de monitoramento constante, pouco percebido pelo usuário, mas desfrutado como recurso pelos operadores do *marketing* digital. Isso porque a potencialidade, ignorada por muitos, das redes e plataformas sociais e digitais, é sustentada por fatores econômicos e comerciais.

A vigilância constante confronta a privacidade, contudo o conceito de privacidade pode ser indefinível, se considerar que cada pessoa pode lhe atribuir um significado, mas todas as pessoas têm algo que não gostariam de expor (Snowden, 2019).

A virtualização da vida por meio das redes sociais, expande a vigilância ao passo que diminui a privacidade. As plataformas de interações sociais são uma vitrine de experimentos comportamentais, e não são desenvolvidas, modificadas e aperfeiçoadas constantemente apenas para entretenimento dos usuários. É preciso compreender que existe um fio econômico por trás do aprimoramento das atividades que são, em verdade, comerciais.

As grandes empresas da tecnologia como *Google*, *Apple*, *Meta*, *Amazon* e *Microsoft*, são as maiores protagonistas da vigilância algorítmica, coletam dados dos seus usuários por meio das mídias sociais, mecanismos de buscas e dispositivos inteligentes, com a finalidade de utilizá-los no direcionamento preciso de anúncios e conteúdos personalizados para cada perfil de usuários,

delineando perspectivas individuais por meio da limitação de acesso às informações diversificadas, e interferindo diretamente na autonomia individual.

O consumidor pode interpretar as sugestões das plataformas digitais de forma benéfica, contudo a coleta de dados pode ser utilizada para manipular os usuários da rede, funcionando, também, como um gatilho para compradores compulsivos (Florêncio, 2019).

As interações e relações interpessoais se dando a quase todo tempo por intermédio das plataformas, permite que essas empresas conheçam profundamente o perfil de seus usuários, podendo segmentá-los a depender do propósito, e a finalidade pode ser convertida para manipulação de interesses políticos.

No ano de 2013, Edward Snowden, ex-funcionário da NSA<sup>25</sup> fez grandes revelações sobre o sistema de vigilância promovido pelo Governo dos Estados Unidos, por meio de monitoramento em massa por meio da coleta de metadados originados em comunicações eletrônicas (Snowden, 2019), o que levanta questões acerca dos limites entre interferência Estatal e segurança pública, que podem impactar diretamente na democracia, quando, por exemplo, utilizada para manipular a opinião pública e política.

A depender dos *layouts* dos aplicativos utilizados, os usuários serão constantemente monitorados, fornecendo de forma contínua uma quantidade exorbitante de dados que poderá servir para traçar um perfil muito bem delineado daquela pessoa, possibilitando desde influências consumeristas às preferências políticas.

As formas como os conteúdos são distribuídos e os critérios embutidos nessa seleção podem não ser justos, embora muitos ainda tentem defender a neutralidade das redes e dos algoritmos, é essencial estabelecer regulamentações robustas que protejam a privacidade dos usuários da internet e assegurem transparência no tratamento de dados pessoais.

O debate sobre vigilância algorítmica envolve discussões éticas, em razão da possibilidade de algoritmos reproduzirem preconceitos decorrentes de vieses (*bias*) discriminatórios no momento em que são programados, ou extraírem uma

---

<sup>25</sup>National Security Agency – NSA é a Agência de Segurança Nacional dos Estados Unidos (Snowden, 2019).

leitura discriminatória a partir de informações como dados históricos que tendem a perpetuar desigualdades e injustiças sociais. A leitura de mundo do algoritmo pode prejudicar liberdades civis e direitos individuais a partir da vigilância excessiva.

A coleta de dados e seu processamento por algoritmo é constante, e levanta questões sobre privacidade, ética e equilíbrio entre segurança e liberdade individual. As empresas de tecnologia precisam trabalhar suas ações para garantir que seus algoritmos não sejam utilizados como veículo de disseminação das discriminações ou preconceitos contra os sujeitos dos dados, e os usuários também carecem de uma melhor consciência do ambiente digital.

#### 4.1 ALGORITMOS

Os algoritmos são códigos com instruções que direcionam as funções de um computador, determinando o que ele deve fazer, isso ocorre por meio da capacidade dos algoritmos denominada por Claude Shannon – o pai da teoria da informação - de “raciocínio”, que se dá por meio da atividade de ligar e desligar, rapidamente, chaves existentes nos computadores, denominadas de “transistores”. Os algoritmos são, então, uma sequência de raciocínio lógico que comanda instruções para uma determinada ação (Domingos, 2017).

Os algoritmos são a base estrutural da computação, podendo ser simples ou inteligentes:

Algoritmos simples ou inteligentes analisam, comparam e tratam informações dos mais variados formatos a todo momento. A principal diferença entre eles é que, enquanto os algoritmos são códigos computacionais escritos para resolver problemas específicos, os algoritmos inteligentes – sejam eles chamados de inteligência artificial ou machine learning – são programados para solucionar problemas (Meireles, 2021).

A inteligência artificial (IA) é um ramo da ciência da computação que surgiu na década de 40, quando neurocientistas e cientistas da computação se inspiraram no sistema neural humano para criar redes de conexões inteligentes, contudo, o termo *Artificial Intelligence* - AI (Inteligência Artificial - IA), só começa a ser utilizado na década de 50, (Russel; Norvin, 2013).

Embora os sistemas inteligentes (IA) sejam extraordinários e tenham sido desenvolvidos a partir da observação do sistema neural, não são uma reprodução mecânica ou artificial do cérebro humano. O ser humano realiza uma busca incessante pela superação de si mesmo, e aprimoramento das capacidades cognitivas e tecnológicas, isso em razão da própria inteligência ser um fator importante na dominação da espécie *homo sapiens*. A busca do homem pela compreensão da mente humana e seus sentidos ocorre há anos, e a IA vai além da própria compreensão, sendo também uma criadora de entidades inteligentes (Russel; Norvin, 2013).

O homem dominou a si mesmo, mas desenvolveu tecnologias que não são, necessariamente, por ele dominadas, como a inteligência artificial, que pode se desenvolver de forma autônoma. Para Tim Wu, (2012, p. 209), a ideia que prevaleceu sobre a forma de utilização dos computadores pelos homens de que eles “seriam usados pelos homens no processo de pensamento, como auxiliares analíticos, e não como calculadoras (o *status quo*), nem como substitutos (a coisa fantasiosa)”, se estende para a relação entre inteligência artificial e homens, uma vez que a IA auxilia e não substitui.

Essa tecnologia foi aprimorada de tal forma que é possível a ela, se autoprogramar, isso porque uma das vertentes da IA, o aprendizado de máquina ou no inglês, *machine learning*, trabalha com algoritmos, que por meio de dados coletados alimentam a capacidade de reproduzir novos algoritmos, sendo uma espécie de programação automática em que eles “descobrem tudo sozinhos” (Domingos, 2017).

Essa forma de desenvolvimento autônoma dos algoritmos, quando eles mesmos criam novos programas, desperta atenção pelo caráter opaco que possui, isso significa que nem mesmo os programadores do código inicial sabem até onde eles irão se autoprogramar, ou quais as possíveis consequências desses futuros modelos matemáticos.

Na realidade atual, se houvesse um colapso e todos os algoritmos fossem extintos, quase nada continuaria em funcionamento. Isso em razão deles serem instrumentos de quase toda tecnologia que se conhece, desde objetos inteligentes aos sistemas de instituições bancárias, companhias aéreas, indústrias, e etc. (Domingos, 2017).

Sendo assim, os algoritmos operam nas mais diversas questões decisórias, que podem ser automatizadas, ou seja, sem interferência direta de um ser humano. Toda liberdade e autonomia dos algoritmos cerceiam essas mesmas características do usuário de tecnologias, como se houvesse uma transferência de um para outro. O homem abre mão de direitos personalíssimos para desfrutar de benefícios tecnológicos.

Para Cathy O'Neil (2020), os algoritmos têm decisões discriminatórias e injustas. A autora que trata do tema “injustiça algorítmica”, ressalta o fato de que os algoritmos são programados por seres humanos, e em sua maioria, esse campo da ciência da computação é dominado por homens brancos héteros.

Se um programador com esse perfil desenvolve um algoritmo, junto com as instruções iniciais estarão embutidos vieses (*bias*) discriminatórios, em outras palavras, as perspectivas desse programador ensejarão futuros preconceitos, seja em razão do sexo ou, por exemplo, de raça, portanto, o algoritmo não será neutro (O'Neil, 2020). Quando um algoritmo com vieses racistas ou machistas, se autoprograma no método de *machine learning*, ele se torna uma ameaça à democracia.

Um exemplo de discriminação algorítmica são as tecnologias de reconhecimento facial, que tendem a ser discriminatórias e embora sejam utilizadas sob o pretexto de uma segurança pública mais democrática, “os jovens, homens e pessoas negras são alvo de maneira sistemática e desproporcional de sistemas de vigilância”, e não em razão de antecedentes particulares ruins, mas por pertencerem a determinado grupo social submetido às consequências de vieses discriminatórios (Norris, 2023, apud Negri; Oliveira; Costa, 2020, p. 93).

Nesse aspecto, a utilização de tais tecnologias se mostra preocupante quando aplicada a um grupo específico de pessoas que podem ser discriminadas sem nenhuma justificativa aparente, que não o preconceito algorítmico.

Não há justiça nem misericórdia nas ações autônomas decorrentes de mecanismos digitais controlados por IA, mas “no que tange a outros animais, os humanos já se tornaram deuses há muito tempo. Não gostamos de refletir sobre isso com muita profundidade porque não somos deuses particularmente justos ou misericordiosos” (Harari, 2016, p. 79), e toda a injustiça humana pode ser impensadamente transpassada aos códigos pelos programadores.

Questões pertinentes aos vieses algorítmicos e a discriminação neles embutida podem se manifestar contra diversos fatores, sendo preponderantemente questões de gênero, raciais e, também, socioeconômicas.

Para O'neil (2020, p. 33), “nenhum modelo consegue incluir toda a complexidade do mundo real ou as nuances da comunicação humana. Inevitavelmente alguma informação importante fica de fora”, e por não ser possível reproduzir em dados todas as questões que permeiam diversas situações, não se pode esperar humanidade e ética nas análises feitas por robôs.

Os algoritmos podem representar ameaças a direitos fundamentais e princípios constitucionais como privacidade, autonomia e igualdade de oportunidades. Tudo em razão da possibilidade de influenciar consumidores e eleitores nos processos decisórios, uma vez que podem submetê-los à mineração de dados e persuasão, ocasionando uma invasão na esfera da privacidade, a partir de uma coleta e tratamento obscuros de dados pessoais ou metadados, atingindo a autonomia da pessoa humana por meio de controle informacional, que gera poder de influência nas decisões a serem tomadas (Marrafon; Coutinho, 2021).

Tudo isso é direcionado de acordo com o *profiling* do usuário, não existe mágica, a *machine learning* funciona por meio de previsões comportamentais que são possibilitadas pela alimentação diária de banco de dados com as mais diversas informações dos usuários, (Domingos, 2017).

Para explicar melhor o que é a *machine learning*, Domingos (2017, p. 30) faz um comparativo com o sistema de agricultura de uma fazenda, nele “os algoritmos de aprendizado são as sementes, os dados são o solo e os programas de aprendizado são as plantas crescidas”. O especialista desse subcampo da inteligência artificial seria o fazendeiro que cuida, mas deixa o processo da plantação se desenvolver normalmente.

A analogia trazida pelo autor, demonstra que a *machine learning* se desenvolve de forma autônoma e quanto mais dados têm acesso, maiores suas possibilidades de aprendizado, podendo assumir diversas formas e ser conhecida por outras denominações como, “reconhecimento de padrões, modelagem estatística, mineração de dados, descoberta de conhecimento, análise preditiva, ciência de dados” (Domingos, 2017, p. 31), e etc.

Compreende-se, então, que *machine learning* não se resume à mineração de dados, sendo elementos distintos que combinam suas técnicas para obter melhores resultados (Silva, 2019). A mineração de dados reconhece padrões e tem sido essencial como técnica de vigilância algorítmica, conseguindo filtrar rapidamente uma quantidade sobre-humana de dados.

## 4.2 MINERAÇÃO DE DADOS E PERFIS

A era da informação e da hiperconexão gerou um volume sem precedentes de dados digitais. Esse excesso de conteúdo precisa de técnicas que consigam fazer uma filtragem de forma rápida, para extrair as informações que realmente importam à determinada finalidade.

A mineração de dados (*data mining*) surge como uma ferramenta eficaz e apta a realizar uma seleção de informações a partir de dados brutos contidos no *Big Data*, por exemplo, com o reconhecimento de relações ocultas entre dados e estabelecimento de padrões (Galvão; Marin, 2008).

A mineração de dados pode ser definida como:

[...] um processo automático ou semiautomático capaz de efetuar uma exploração analítica de grandes bases de dados, com o intuito de descobrir padrões essenciais na assimilação de informações importantes e oferecer suporte à geração de conhecimento (Silva; Peres; Boscarioli, 2016, apud Rossini, *et al.*, 2018).

É preciso compreender que nem todo “dado” pode ser chamado de informação, pois o “dado bruto” não traz por si só informações, mas a partir do tratamento direcionado, tem-se a interpretação que dá significado ao “dado”, e a mineração dos dados extrai informações (Rossini, *et al.*, 2018).

Empresas públicas e privadas promovem coletas de dados constantemente, além da hiperconexão dos usuários da rede, utilização de *Wearables* e objetos inteligentes, que constroem uma extensão de dados impossível de ser submetida à apreciação humana. Tecnologias como a mineração de dados ajudam a “separar o joio do trigo”.

A maior compreensão dos computadores em relação à linguagem humana, aliada à capacidade de processamento rápido de dados, potencializa a

inclinação para uma sociedade de decisões automatizadas (O'Neil, 2020) e diante da automatização de decisões, levanta-se, novamente, questões sobre privacidade, a interferência algorítmica nas esferas individuais e os riscos do extrapolamento dos limites individuais.

Para uma melhor compreensão da mineração de dados, tem-se, então, uma diferenciação entre dado, informação e conhecimento, no qual:

[...] os dados podem ser interpretados como itens essenciais que são captados e armazenados por ferramentas da Tecnologia da Informação, com a finalidade de expressar fatos do mundo real de forma a serem aplicados no meio computacional. As informações representam os dados processados e, para isso, diversas ferramentas da Tecnologia da Informação também são utilizadas. O conhecimento corresponde a um padrão ou conjunto de padrões, através do qual dados e informações podem ser relacionados (Goldschmidt; Passos; Bezerra, 2015, apud Rossini, *et al.*, 2018).

Os dados coletados, por si só, não apresentam riscos significativos. Considerando então, esses dados dentro de um imenso banco de dados, isolados, não refletem a vigilância algorítmica. Os riscos da vigilância se representam nas possibilidades de conhecer e segmentar os dados de um indivíduo ou de um grupo de indivíduos.

Na área da saúde, a coleta de dados tem por finalidade, especialmente, a busca por conhecimento, contudo também é utilizada para relacionar informações presentes em bancos de dados, o que pode ser benéfico em muitas situações (Galvão; Marin, 2008), mas também pode desencadear discriminações e invasão à privacidade, a depender de como essas informações serão tratadas e com quem serão compartilhadas. Um histórico médico individual e familiar de determinado paciente, nas mãos de uma empresa de plano de saúde, por exemplo, pode interferir no valor da mensalidade que determinado paciente desembolsa para utilizar o serviço.

Uma forma muito contínua de alimentação de dados e aprendizagem de máquina são as postagens de fotos nas redes sociais. Quando a plataforma é capaz de identificar as pessoas que estão na foto e indicar quais são suas respectivas contas, e quando a máquina erra ou não é capaz de identificar determinada pessoa, o próprio usuário que postou a foto pode selecionar o perfil

da conta de seu amigo. Dessa forma, o algoritmo aprende quem é quem (Rossini, *et al.*, 2018).

A mineração de dados pode relacionar dados de um usuário com seus amigos de conexões mais frequentes, e fazer, por exemplo, uma correlação de gostos comerciais ou preferências políticas, a partir de padrões identificados. Além disso, a técnica pode ser utilizada nas mais variadas áreas, desde a educação até o setor público ou privado, sendo extremamente útil nas necessidades de processamentos de grandes bancos de dados.

As técnicas elaboradas de direcionamento de conteúdo pelas tecnologias inteligentes são possibilitadas pelo excesso de dados que são fornecidos continuamente e a consequente datificação da personalidade.

Os modelos como as tecnologias e as comunicações foram se desenvolvendo também influenciam a coleta e processamento de dados:

A propagação do uso dos sistemas algoritmos que aprendem com dados propiciou a emergência dos modelos de negócios orientados a dados (data-driven business models), do *marketing* dirigido por dados (data-driven *marketing*), governança baseada em dados (data-driven governance), entre outros (Silveira, 2020, p. 2).

O desfrute das facilidades da sociedade da informação exige que a pessoa exponha seu “eu” com “consequências que vão além da simples operação econômica e criam uma espécie de *posse permanente* da pessoa por parte de quem detém as informações a seu respeito” (Rodotà, 2008, p. 113). Os danos colaterais da exposição cibernética vão de manipulações de padrões de consumo até ao uso político das informações do indivíduo, com a vigilância se espalhando de forma fluida pela vida dos usuários da internet.

Dentre as mais expressivas fontes de coletas de dados na rede, estão, “as transações comerciais, os censos e registros públicos, as pesquisas de mercado e de estilo de vida, sorteios e concursos, a comercialização e cessão de dados, e as tecnologias de controle na internet” (Mendes, 2014, p. 96, apud Lima, 2019, p. 34).

O indivíduo hiperconectado, permanentemente nas redes, está submetido ao *layout* de monitoramento, em outras palavras, as redes são configuradas para perfilar seus movimentos, seus hábitos de consumo, sua rotina, sua rede de

contatos, invadindo e limitando a esfera da autonomia individual (Rodotà, 2008, p. 19).

Diversas são as técnicas que podem ser aplicadas no tratamento dos dados brutos coletados pelas tecnologias e dispositivos inteligentes, dentre elas o *Profiling*, que consiste na interpretação de dados que formam um perfil comportamental de um indivíduo ou de um grupo específico a partir da síntese de seus hábitos e preferências pessoais (Doneda, 2019).

O *profiling* também pode ser definido como uma decisão algorítmica que tem “[...] como resultado a elaboração de conjuntos de informações bastante estruturadas ou ‘definição de perfis’, capazes de permitir análises e previsões de comportamentos e até de atitudes morais do interessado” (Florêncio, 2019, p. 247).

O *profiling* está fortemente ligado às técnicas de *data mining* (mineração de dados), que por sua vez é uma técnica “que consiste em descobrir e extrair padrões e comportamentos não triviais em grandes conjuntos de dados. Esses padrões descobertos podem servir como meio de análise e podem ser utilizados para previsão de comportamentos e decisões” (Lima, 2019, p. 37).

A mineração de dados pode trabalhar os dados repetindo padrões discriminatórios de antigos tomadores de decisão ou representando discriminações visualizadas na sociedade, podendo reproduzir desigualdades a partir da observação de outros dados. “A mineração de dados, desde a sua coleta até a apresentação de um resultado, pode se utilizar de cinco mecanismos que podem levar a distorções: definição do problema, treinamento dos dados, seleção de dados, utilização de *proxies* e *masking*” (Barrocas; Selbest, 2016, apud Braga, 2019, p. 681).

Na utilização da técnica de mineração de dados, pode-se utilizar, 1. A mineração descritiva de dados, que busca relacionar (não explicar) objetos de um banco de dados e obter informações; e 2. A mineração preditiva de dados, que a partir de padrões busca prever resultados/ eventos (Lima, 2019).

Na prática, “se um indivíduo possui um carro de grande porte, mas não tem filhos, pode existir uma suposição de que o dono do veículo está acima do peso” (Florêncio, 2019, p. 223). As implicações jurídicas surgem com o repasse dessas informações para terceiros, como planos de saúde, impactando na precificação do serviço pra aquele usuário.

Em uma pesquisa recente, o Symantec<sup>26</sup> expõe que aplicativos de *zero-price advertisement business model*, disponíveis para *Android* e *IOS*<sup>27</sup>, podiam solicitar permissões invasivas, captando informações excessivas e pessoais dos usuários, como geolocalização, acesso às câmeras, conteúdos de mensagens do celular e registro de chamadas telefônicas (Florêncio, 2019, p. 263), o que deixa os usuários extremamente vulneráveis, especialmente por não se ter uma cultura de ler termos de serviços ou monitorar configurações de privacidade dos *smartphones*.

Os serviços *zero-price advertisement business model*, como narrado antes, trabalham com uma ampla coleta de dados de usuários, possibilitando a criação de perfis que servirão, por exemplo, para direcionar conteúdos futuros para o usuário, recomendar produtos, exibir anúncios e publicações.

O reflexo do *profiling* enquanto um problema da datificação da personalidade é o fato de que no universo eletrônico, o indivíduo será representado por aquele perfil, de modo que os entes com quem as interações se deem por meio virtual, só conhecerão aquela parcela da pessoa, diminuindo sua liberdade em razão da compreensão de que é possível conhecê-la por inteiro a partir de uma fração de comportamento pré-definido (Doneda, 2019).

As implicações do *profiling* digital são refletidas no direcionamento de conteúdo ao usuário, com a consequente limitação das possibilidades de ampliação de liberdades individuais, autonomia, expressão do pensamento, aprisionando o indivíduo em bolhas de filtro (Bauman; Lyon, 2013). Nessa perspectiva, “os aplicativos de IA influenciam as informações que você vê online, prevendo qual conteúdo é atraente para você, capturam e analisam dados de rostos para aplicar leis ou personalizar anúncios” (ABCD USP, 2023, recurso *on-line*).

Além da afetação das perspectivas exclusivamente individuais, as técnicas de direcionamento de conteúdo podem ser expandidas para situações amplamente discriminatórias, como concessão de crédito e taxas de juros, exclusão em processos seletivos. Dentre os riscos que os algoritmos podem trazer estão a “manipulação, viés, censura, discriminação social, violações da

---

<sup>26</sup> Empresa de segurança da informação.

<sup>27</sup> Sistema operacional móvel da Apple.

privacidade e dos direitos proprietários, abuso do poder de mercado, efeitos sobre as capacidades cognitivas e uma crescente heteronomia” (Doneda; Almeida, 2016, recurso on-line).

Na vigilância algorítmica a mineração de dados e as técnicas de *profiling* podem ser utilizadas de forma capciosa, com a finalidade de manipular a acessibilidade de um usuário a determinado conteúdo de acordo com seu perfil, limitando suas escolhas e sua visão de mundo.

#### 4.3 METADADOS – RASTROS DIGITAIS

Os metadados, são os resíduos da vida digital que podem ter sua coleta como imperceptível, mas dispõem de muitas informações importantes e capazes de viabilizar o rastreio da vida digital.

A problemática da pouca valorização dos metadados se dá pelo fato dos usuários da internet guardarem preocupação apenas com o conteúdo bruto, pessoal e íntimo das informações trocadas e armazenadas, como se a vigilância algorítmica se importasse, por exemplo, com os textos escritos, fotografias tiradas, informações trocadas em uma ligação (Snowden, 2019).

As informações que são trocadas e transmitidas, têm valor além do conteúdo privado que preocupa a maioria das pessoas:

[...] Mas a lamentável verdade é que o conteúdo de nossas comunicações raramente é tão revelador quanto seus outros elementos – as informações não escritas e não ditas que podem expor o contexto e os padrões mais amplos de comportamento. A NSA chama isso de metadados. O prefixo do termo, *meta*, que tradicionalmente é traduzido como “acima” ou “além”, aqui é usado no sentido de “sobre, acerca de”: metadados são dados sobre dados. Mais exatamente, são dados feitos por dados – um punhado de tags e marcadores que permitem que os dados sejam úteis. A maneira mais direta de pensar nos metadados, no entanto, é como dados de atividade: todos os registros de tudo que você faz em seus dispositivos eletrônicos e tudo que eles fazem por conta própria. Você faz uma ligação telefônica, por exemplo: seus metadados podem incluir a data e a hora dessa ligação, a duração, o número de origem da chamada, o que está sendo chamado e a localização de ambos. (Snowden, 2019, p. 156).

Metadados são, então, informações contidas dentro das informações que comumente os indivíduos preocupam em proteger. As pessoas parecem se preocupar mais com a exposição negativa da figura pessoal e com o que pode ser gerado a partir de algum comportamento íntimo ou social, do que de fato com a segurança dos seus dados pessoais. É como se estivessem presas, em sua maioria, no conceito primário de privacidade que dispunha sobre o “ser deixado só” e “não ter a esfera pessoal exposta”, do que propriamente com o conceito trabalhado por Rodotà (2008) de ter “controle do que é feito com os dados pessoais coletados”.

O elemento metadado pode, também, ser apresentados como “como matéria-prima que pode ser analisada e processada em algoritmos preditivos sobre o comportamento humano futuro – ativos valiosos na indústria de mineração” (Dijck, 2017, p. 46).

Os usuários da internet não desenvolveram, no geral, uma reflexão de grupo social no que se refere a padrões de comportamento, e tendem a pensar, isoladamente, nos dados que compartilham, nas conversas ou mensagens que não querem ver expostas, assim como o histórico de navegação, sem projetar a ideia de que o comportamento praticado importa mais do que os fatos isolados, e pode servir para classificá-las, perfilá-las, e manipulá-las, com finalidades diversas – comerciais, políticas e outras ainda desconhecidas.

Os metadados podem conter informações como qual o tipo de equipamento utilizado (o que pode revelar padrão de consumo e condição econômica), o lugar de onde foi feito o acesso, se de um bairro nobre ou da periferia, por exemplo, quando foi enviada determinada mensagem, demonstrando o tipo de rotina do indivíduo, podendo revelar se tem hábitos noturnos, se tende a realizar compras fora do horário comercial, etc. Assim como o destinatário de uma mensagem ou ligação pode dizer sobre as conexões interpessoais de determinada pessoa, além dos dados de georreferência de um usuário, passando por todos os lugares onde esteve e onde se conectou (Snowden, 2019).

Metadados são dados produzidos sem a possibilidade de controle por parte de quem os fornece. Você pode se encontrar na cidade de São Paulo e realizar uma ligação dizendo estar na cidade do Rio de Janeiro, o que você diz está sob seu controle, mas os metadados dessa ligação demonstram sua

localização exata, seja na utilização das torres de celular ou pela conexão de internet, não é possível controlar todos os dados produzidos.

Os metadados estão relacionados ao comportamento humano e são subjetivos, precisando de uma análise que os compreenda. As técnicas para compreensão do comportamento, a partir da interpretação dos metadados, são constantemente aperfeiçoadas para captar o valor embutido nos “dados brutos” (Dijck, 2017).

As legislações parecem se preocupar mais com a temática dos dados pessoais do que com os metadados, o que pode afastar as normativas da realidade tecnológica em relação à proteção da privacidade e das comunicações. O fato de as agências de inteligência se preocuparem mais com metadados do que com os dados pessoais em si, deveria ser um ponto de atenção legislativo. Os metadados facilitam a segmentação de usuários em grande escala e a previsão de comportamentos, eles “podem dizer a quem o monitora praticamente tudo que ele quer ou precisa saber sobre você, exceto o que realmente está se passando dentro da sua cabeça” (Snowden, 2019, p. 157).

Os metadados que já foram considerados “subprodutos inúteis”, vêm se tornando um recurso valioso para o maior conhecimento dos usuários das plataformas digitais. “As plataformas de mídia social, ao mesmo tempo, medem, manipulam e monetarizam o comportamento humano on-line” (Dijck, 2017, p. 44 - 45).

Os dados residuais influem grandemente nas técnicas de vigilância algorítmica, quando os usuários expõem informações por meio de dados que não imaginam estar disponibilizando, mas determinam grande parte de sua vida digital. A arquitetura das redes digitais parece ter sido pensada já sob um olhar de monitoramento, devido ao excesso de informações coletadas que se chocam com qualquer mínimo direito à privacidade.

#### 4.4 CAPITALISMO DE VIGILÂNCIA: A ECONOMIA DA ATENÇÃO

Como todo contexto jurídico, as relações de consumo também vêm se modificando ao longo dos anos, alcançando na atualidade dos moldes digitais, proporções jamais vivenciadas. O consumidor e os objetos de consumo já não são mais os mesmos, houve uma migração do consumo, no qual os objetos eram

adquiridos por necessidade ou funcionalidade, para um cenário de consumismo, neste sendo que os bens adquiridos, algumas vezes, sequer possuem uma finalidade.

Primeiro, foram introduzidos os cartões de crédito no meio consumerista, e então, ainda que não se tivesse o dinheiro em mãos para adquirir um bem, era possível optar pelo parcelamento, de forma que o cliente pudesse consumir a partir de um meio aparentemente facilitador, (Bauman, 2008).

Antes, as redes sociais, *e-commerces*, *internet banking* e etc. não eram utilizados na escala atual, portanto a produção de dados era ínfima quando comparada ao que é hoje, condição em que os cartões de crédito deixaram de ser novidade, tornando-se um fio condutor do endividamento. As *fintechs* e seus cartões digitais de fácil acesso, expandiram ainda mais as possibilidades de compras, e com a expansão das possibilidades, houve aumento na coleta de dados, inclusive financeiros.

O direcionamento de conteúdo e vigilância algorítmica podem influenciar consumidores compulsivos a realizarem compras quando se encontram vulneráveis (Florêncio, 2019) e os cartões de crédito permitem que a impulsividade aliada ao imediatismo leve o consumidor compulsivo a um comportamento financeiro autodestrutivo, por meio da aquisição de bens que não correspondem às suas reais condições financeiras.

As interações tecnológicas podem atuar amplificando o cenário consumerista a partir da indicação de produtos e anúncios personalizados, permitidas em decorrência de um amplo conhecimento do perfil de cada indivíduo que, por sua vez, ocorre em razão da datificação da personalidade. Os algoritmos de publicidade predatória podem identificar, inclusive, que determinado usuário se encontra em dificuldades financeiras, passando a lhe oferecer, por meio de anúncios, empréstimos com juros abusivos (O'Neil, 2020).

O capitalismo de vigilância se configura quando o excesso de dados comportamentais, coletados durante a navegação, transforma a conexão digital em um universo comercial, em que a experiência humana é tida como matéria-prima, e os dados coletados, ora são utilizados para aprimorar produtos e serviços no ambiente virtual, ora para configurar o “superávit comportamental” do usuário, tido como fonte de dados. Essa alimentação de sistemas com dados comportamentais, possibilita os “produtos de predição”, que atuam como uma

previsão comportamental dos indivíduos, e são monetizados nos “mercados de comportamentos futuros”, em decorrência do interesse de muitas empresas em valorizar, como forma de aposta econômica que tem funcionado, as ações futuras dos usuários da internet (Zuboff, 2020).

Um grande volume de dados é fornecido por indivíduos de toda parte do mundo, a todo momento, pelos mais diversos meios de coleta de dados, desde o fornecimento de CPF no momento de uma compra, até os dados biométricos de reconhecimento facial, quando se é gravado por algum sistema de segurança, ou os metadados, que são dados sobre dados, em outras palavras, rastros digitais.

As pessoas também utilizam, com frequência, dispositivos inteligentes, sejam eles conectados ao corpo como os *smartwatches*, ou equipamentos domésticos como aspiradores de pó que podem reconhecer e armazenar os espaços físicos da casa, ou, ainda, dispositivos inteligentes com captação de voz e sons ambiente, como a *Alexa*<sup>28</sup>.

Os algoritmos de vigilância, por meio do grande conjunto de dados, ou *Big Data*, promovem uma máquina de publicidade *on-line*, onde é possível direcionar a publicidade para o consumidor-alvo através do fornecimento de dados por ele próprio, sendo possível aos anunciantes saber a hora certa para abordagem comercial (O'neil, 2020).

A utilização desprezensiosa de tecnologias de vigilância, faz com que usuários de toda parte do mundo forneçam “gratuitamente” seus dados, se tornando o objeto de onde as empresas extraem e estudam perfis comportamentais, em outras palavras, os consumidores tornam-se produtos, sendo a “matéria-prima gratuita” que movimenta o ciclo dos dados (Zuboff, 2020).

A vigilância deve, então, ser encarada como consequência do comportamento dos indivíduos, que deixa um rastro de informações alcançada por meio de algoritmos e aplicada de forma universal e não isolada, e considera-se, ainda, que os maiores riscos na coleta de dados ocorrem por meio das empresas privadas e não das instituições públicas (Rodotà, 2013).

---

<sup>28</sup> Assistente virtual desenvolvida pela *Amazon*.

A previsibilidade do comportamento humano, oriunda da vigilância extrema vivenciada no ambiente hiperconectado, tem um valor de mercado elevado e muitas empresas querem pagar por isso. Durante a implementação do modelo de mercado vigilante:

O *Google* foi o pioneiro do capitalismo de vigilância na concepção e na prática, nos recursos inesgotáveis para pesquisa e desenvolvimento, além de pioneiro em experimentação e implementação, porém não é mais o único ator seguindo esse caminho. O capitalismo de vigilância logo se espalhou para o *Facebook* e depois para a *Microsoft*. [...] Como pioneiro do capitalismo de vigilância, o *Google* lançou uma operação de mercado sem precedentes nos espaços não mapeados da internet, onde enfrentou poucos impedimentos jurídicos ou de concorrentes, como uma espécie invasora num ambiente livre de predadores naturais. Seus dirigentes conduziram a coerência sistêmica de seu negócio num ritmo temerário, que nem instituições públicas nem indivíduos conseguiram acompanhar (Zuboff, 2020, p.20).

O *Google* não só foi pioneiro no capitalismo de vigilância, como está respondendo um processo histórico, relativo à formação de truste, decorrente do monopólio promovido por ele no ambiente digital, onde seu motor de busca está relacionado a possíveis práticas concorrenciais abusivas. O processo em questão, intitulado “Estados Unidos v. *Google*” investiga o *Google* pela suposta violação da lei antitruste do país por meio de acordos entre a plataforma e empresas de tecnologia, como Apple e outras fabricantes de *smartphones*, para que os usuários dessas empresas utilizassem o motor de busca *Google*. O julgamento histórico foi marcado para 09 de setembro de 2024 (Spadoni, 2024).

Já o Instagram, da empresa *Meta* (antigo *Facebook*), é uma plataforma de mídia social extremamente difundida no Brasil e capaz de captar muitos dados de seus usuários. O aplicativo serve para compartilhar imagens, vídeos, dispondo também, de um chat para interação dos usuários. O Instagram é uma plataforma que se utiliza do capitalismo de vigilância, monitorando seus usuários através da análise de um amplo fornecimento de dados (Zuboff, 2015, apud Bentes, 2018).

As plataformas digitais tornaram-se mecanismos que movimentam a economia através da atenção que o usuário dedica à sua utilização, e das ações que ele pratica enquanto conectado. Essa atenção e ação fornecem ampla

informação sobre os usuários, possibilitando que as empresas detenham maior controle na manipulação dos comportamentos, atendendo à finalidade comercial (Zuboff, 2020).

A economia da atenção se relaciona com o excesso de conteúdo disponibilizado, por não ser possível acessar todas as informações dispostas diariamente, devendo escolher quais as mais interessantes. As tecnologias persuasivas buscam atrair os espectadores no menor tempo possível e quanto mais tempo for dedicado às plataformas, mais a atenção será monetizada:

[...] o mercado de dados digitais atualmente está intimamente relacionado às operações da Economia da Atenção. A premissa fundamental de uma economia atencional é que, em um mundo onde há uma oferta infinita de conteúdos, produtos, informações e imagens, o que falta é a atenção (e tempo) para consumir todas essas ofertas. Assim, enquanto um recurso cada vez mais escasso, a atenção se torna cada vez mais valiosa nesse contexto (Bentes, 2018, recurso on-line).

Com tanta informação e recursos disponíveis, a mineração de dados serve de instrumento para determinar que um conteúdo seja exibido para um usuário que nele tenha interesse, ou que possa vir a ter. Para o correto direcionamento de conteúdo, o algoritmo precisa conhecer as preferências do usuário e esse conhecimento também se relaciona com a atenção dedicada às redes.

A economia baseada em dados precisa ter sua fonte alimentada, e para isso, as empresas de tecnologia trabalham técnicas persuasivas para que seus usuários permaneçam mais tempo conectados e navegando em suas plataformas. Para além da relação atenção/tempo na economia da atenção, existe, também, uma relação entre vigilância e espetáculo, quando de um lado se tem o monitoramento e distribuição persuasiva de conteúdo pelas redes sociais, e de outro tem-se as formas como o usuário é visto enquanto ser e em suas relações com os outros (Bentes, 2018).

Analisa-se a vigilância sobre três prismas, 1. O de finalidade comercial, quando o conhecimento de um perfil de usuário pode levar às manipulações consumeristas por meio de sugestões de produtos, direcionamento de anúncios, dentre outras formas que interferem na autonomia do usuário; 2. O político, quando o usuário se configura como um consumidor de informações, e um

conhecimento aprofundado dos cidadãos usuários de mídias digitais pode conduzir conteúdos, manipulando opiniões políticas e interferindo nas democracias, e 3. O controle estatal, quando o próprio governo pode manipular dados, como nos sistemas de segurança pública com monitoramento por reconhecimento facial, incidindo em questões discriminatórias que se chocam com direitos humanos fundamentais.

## 5 CONSUMO DE INFORMAÇÕES POLÍTICAS E DESINFORMAÇÃO

As formas de poder se desenvolveram em diversas camadas da sociedade ao longo dos anos, assim também, as formas de influenciar os indivíduos foram se modificando. Os meios de comunicação passaram pela mídia impressa, telégrafo, rádio, cinema, TV, telefone fixo, e a internet (Wu, 2012), sendo que desde a mídia impressa já eram utilizadas manobras de desinformação.

A política e a internet são instrumentos de poder, a primeira enquanto forma de governo e a segunda como meio atualmente utilizado para alcançar formas de controle, como determinado governo. Ambas são estruturadas a partir da retórica e persuasão, visando direcionar o discurso e manipular comportamentos dos receptores.

A internet, então, teve em sua popularidade enquanto meio de comunicação massiva, possibilidades de expansão de conteúdo, especialmente com a popularidade dos *smartphones* que propiciou mobilidade e maior conectividade e, portanto, maior alcance dos conteúdos. As plataformas digitais não são mecanismos recentes de comunicação, mas sua expressividade sim.

A internet se tornou mais acessível, e seu acesso massivo foi possibilitado pelos novos moldes de comunicação incorporados pelas TICs<sup>29</sup>, com uma interação em rede mais rápida e novas dinâmicas políticas, como as possibilidades dos usuários de interagir com os conteúdos, comentando as notícias (Penteado, *et al.*, 2011).

A um clique, estão as interações sociais, redes de contatos amigos e desconhecidos, nas quais é possível postar, interagir e compartilhar conteúdos em tempo real. Ideias, palavras e imagens se espalham de maneiras que antes eram pouco imaginadas por muitos, possibilitando um alcance mundial em segundos.

A forma como a política se beneficia dos atuais moldes de comunicação, por meio das plataformas digitais, é uma questão que vai além do cenário jurídico, envolvendo temáticas sociais, tecnológicas, psicológicas e de consumo.

---

<sup>29</sup>Tecnologias da Informação e da Comunicação; máquinas e programas que geram o acesso ao conhecimento.

O que foi originalmente desenvolvido para comunicação social e com finalidade comercial, se expandiu para áreas como a política, em razão de sua eficácia e influência.

É possível, construir a imagem de um candidato na internet de forma mais eficiente do que na TV, uma vez que o tempo de divulgação de propostas é ilimitado, e seus eleitores também podem fazer campanha por ele de forma contínua. Visualiza-se pessoas debatendo sobre política e propagando conteúdos sobre seus candidatos e respectivos oponentes em tempo real (Pinheiro, 2021).

A internet não é a vilã, o contexto depende de como os usuários utilizam o canal de comunicação em seu potencial político. Deve-se considerar o acesso que as pessoas têm à informação digital e sua capacidade de entendimento das notícias que recebem; a cultura política como a participação dos cidadãos de forma ativa; e as características da sociedade do espetáculo, que “causam barulho”, mas não necessariamente comunicam, podendo, inclusive, desinformar, empobrecendo os debates (Penteado, *et al.*, 2011).

Com a migração da política para os meios digitais, as *fake news* e a desinformação acerca da temática também se potencializaram. Portanto, com o excesso de exposição às mídias sociais e à internet de forma geral, o juízo de valor dos usuários da rede ficou prejudicado pelo volume de informações e sua movimentação de forma acelerada.

Na política moderna, o termo *fake news* ficou mais conhecido e muito utilizado a partir das eleições do ex-presidente *Donald Trump*, em 2016, nos Estados Unidos e do escândalo de espionagem política da *Cambridge Analytica*. Já no Brasil, a eleição de Bolsonaro<sup>30</sup>, em 2018, foi marcada pelas *fake news*, assim como todo o seu mandato, e em 2022, com a possibilidade de elegibilidade do candidato Luís Inácio Lula da Silva, atual presidente do Brasil<sup>31</sup>, também foi possível visualizar a expressiva materialização do debate político inflamado, nos ambientes digitais, quando uma nova disputa acirrada pelo poder foi travada nas eleições entre Bolsonaro e Lula.

---

<sup>30</sup>Jair Messias Bolsonaro, eleito como presidente da República do Brasil (Senado), mandato: 2019 – 2022.

<sup>31</sup>Luís Inácio Lula da Silva assumiu seu terceiro mandato como presidente da República do Brasil em janeiro de 2023 (Senado, 2022), mandato: 2023 - 2026.

A discussão da política no cenário virtual se torna importante frente aos contornos dados ao direito digital na atualidade. Embora tenham sido implantadas limitações, de acordo com o desenvolvimento social do virtual (Pinheiro, 2021), ainda não há legislação eficaz no combate e prevenção da desinformação, talvez pelo fato de os fatores mais relevantes, nesses casos, serem subjetivos e de difícil controle, como a educação digital e valores éticos e morais.

Hoje, a utilização da política digital é extremamente expressiva, tendo ganhado atenção de acordo com as novas possibilidades virtuais. Acerca da temática do impulsionamento de conteúdos, a resolução 23.732 de 2024 que alterou a de n.º 23.610 de 2019 regula a propaganda eleitoral das eleições e determina que poderá ocorrer desde que:

- I - o serviço seja contratado por partido político ou pela pessoa natural que pretenda se candidatar diretamente com o provedor de aplicação;
- II - não haja pedido explícito de voto;
- III - os gastos sejam moderados, proporcionais e transparentes;
- IV - sejam observadas as regras aplicáveis ao impulsionamento durante a campanha (Brasil, 2024).

Nos modelos atuais de propagação de informações políticas atingem até mesmo aqueles que não desejam receber conteúdos políticos, assim é possível ao candidato chegar em um público muito amplo.

A utilização de redes sociais para expandir a política foi aplicada de forma capciosa pela *Cambridge Analítica*, e outras empresas de *marketing* político, e seus métodos serão vistos de forma mais detalhada nos tópicos seguintes, expondo como as empresas se utilizaram de dados pessoais e desinformação para construir um modelo de persuasão que melhor favorecesse seus candidatos.

## 5.1 FAKE NEWS E DESINFORMAÇÃO

Nesse cenário de diálogos inflamados e respostas imediatas, o grande desafio é acalmar os discursos de ódio e compartilhamento de notícias falsas (*fake news*), que influenciam fortemente as opiniões políticas considerando que

a mídia digital propaga conteúdos de forma instantânea que se espalham rapidamente.

É importante dizer que a manipulação experimentada no ambiente digital não é concretizada apenas por meio das *fake news*, mas por notícias estratégicas que influenciam nas ideologias políticas e sociais dos usuários da rede que “é o combustor da era da informação” (Bernardi, 2020, p. 21).

A manipulação de informações e as desinformações já aconteciam na época da mídia impressa, no rádio e na TV. A *Western Union*<sup>32</sup> atuou na manipulação de informações políticas jornalísticas, através da *Associated Press*<sup>33</sup>, para promover *Rutherford Hayes* à presidência dos Estados Unidos (1876), manipulando as perspectivas dos eleitores, por meio de divulgação e omissão de informações a depender do que favorecesse o candidato (Wu, 2012).

Com a massificação de conteúdo experimentada por meio das mídias digitais, o ambiente virtual tornou-se palco da rapidez de espalhamento de notícias e ausência de confirmação de sua veracidade. A sensação de anonimato presente na internet é um elemento favorável ao compartilhamento indiscriminado dessas informações.

As notícias falsas não são novidade, mas o termo *fake news* ganhou muita notoriedade no ano de 2018, no cenário político brasileiro, podendo ser “originalmente entendida como falsificação, manipulação, informação mentirosa” (Waack, 2020, p. 225). É necessário ir além da tradução da palavra para entender o significado de *fake news*, uma vez que sua implicação jurídica transcende a mentira.

Trazendo uma visão mais concreta, entende-se que o direito não se ocupa com as mentiras ditas e espalhadas em qualquer mídia, física ou digital, mas sim com o impacto causado por elas, em outras palavras, cuida do dano subjacente das *fake news*, e observa, ainda, a intenção de quem a propagou (Rais; Sales, 2020).

O que hoje é conhecido por *fake news* são os institutos jurídicos da calúnia, injúria, difamação e desinformação. Em outras palavras, denomina-se popularmente como notícia falsa o que às vezes pode ser uma notícia

---

<sup>32</sup>Empresa de telégrafo, principal inimiga da Bell (Wu, 2012).

<sup>33</sup>1870 - Única fonte de notícias “instantâneas” à época (Wu, 2012, p. 32).

aparentemente verdadeira, mas que tem um caráter e intenção de desinformar, distorcer a realidade ou prejudicar uma imagem e reputação (Waack, 2020).

O cenário de manipulação política conhecido recentemente pode ser na verdade, entendido como *desinformação*, do inglês *desinformation*, que seria além de uma notícia falsa, mas uma informação que tem o intuito de desinformar, confundir, persuadir. O termo *fake news* é empregado de forma errônea nos casos de manipulação política, quando se tem uma notícia verdadeira distorcida, sendo em verdade, *desinformação*.

Os termos *misinformation* e *desinformation* são vinculados às *fake news*, como se tudo fosse visto como notícias falsas, mas em verdade, existem desdobramentos, sendo que *misinformation* de fato é uma notícia falsa, mas não havia nela o elemento da culpa por quem a divulgou, é uma informação incorreta que foi divulgada sem intenção de confundir ou persuadir qualquer ideia, a *misinformation*, não tem uma tradução precisa, mas é a *fake news* que não tinha intenção maliciosa, como uma notícia publicada de forma incorreta, mas sem intenção de causar dano. Já *desinformation* é o que vemos com frequência no cenário político, com intenção de manipular, desinformar e influenciar nas opiniões sobre determinado assunto (Bernardi, 2020).

Entende-se que notícias compartilhadas em grupos de redes sociais com cunho político, invalidando algum candidato, atribuindo-lhe qualquer fato mentiroso, distorcendo de alguma forma a realidade, são *desinformação*. A *desinformação* vai além de uma simples notícia falsa ou mentirosa, ela mascara os fatos de forma a manipular o entendimento do receptor da mensagem, o persuadindo de alguma forma.

É preciso compreender que uma notícia falsa, por si só, não causaria impactos tão grandes quanto a distorção maliciosa dessa mentira, que é a *desinformação*.

## 5.2 RECEPTIVIDADE DAS NOTÍCIAS

Para entender melhor como as notícias falsas são tão facilmente compartilhadas e a credibilidade que lhes é atribuída, é preciso refletir sobre os processos cognitivos dos usuários das redes sociais, que estão expostos às notícias.

O pesquisador Daniel Kahneman, autor do *best seller* “Rápido e devagar: duas formas de pensar”, identificou que nosso sistema cognitivo nem sempre processa as informações com atenção, a maior parte delas são recebidas e processadas de forma automática e intuitiva, sem que haja uma reflexão maior sobre o conteúdo, denominado pelo autor de *efeito halo* (Bernardi, 2020).

Um fator associado ao *efeito halo* pode ser o estado “automático” em que as pessoas se encontram no ambiente hiperconectado. Enquanto os dispositivos digitais dispõem cada vez mais de sensores, os usuários das tecnologias parecem sofrer uma diminuição de sentidos. A rotina acelerada colabora com a vida no “automático”, assim como a acessibilidade de informações, que têm tornado as máquinas cada vez mais inteligentes e os seres humanos mais preguiçosos.

A receptividade dada pelo usuário das redes sociais às notícias falsas ou de alguma forma manipuladas, pode ocorrer em razão de alguma vulnerabilidade intelectual decorrente da busca por atalhos cognitivos, quando não se realiza um processo amplo de análise de informações recebidas e sua procedência. Esse meio de receptividade (*efeito halo*), também pode ser denominado por “avareza cognitiva”, que se refere ao processo automático de raciocínio que não dá atenção aos detalhes e faz um rápido julgamento de certo e errado, como por exemplo, quando a mensagem é enviada por alguém de confiança do receptor (Shane, 2020).

Apesar de o *Facebook* ser extremamente popular nas questões de vazamentos de dados e escândalos políticos por meio de suas estratégias de *marketing*. No Brasil, a relação de confiabilidade no conteúdo das notícias, ocorreu no aplicativo do *Whatsapp*, que foi muito utilizado para comunicações pessoais privadas ou em grupos, como uma forma de continuação do discurso político (Baptista, *et al.*, 2019).

As lentes lançadas sobre as mídias sociais ganharam atenção quanto ao campo da polarização política, por meio das desinformações e *fake news* interferindo na esfera pessoal do indivíduo, e as possibilidades de vigilância que podem impactar na democracia (Felipe, 2022).

Nas redes sociais, como o *Facebook*, o processo automático de raciocínio fica prejudicado pelo excesso de conteúdo a que se tem acesso diariamente. Outra prejudicial é a denominada “dissonância cognitiva”, quando a informação

vai de encontro às certezas do leitor, sendo comum manter-se na zona de conforto entendendo por falsas as notícias, seguindo a mesma lógica de quando viés de confirmação atesta a veracidade de notícias que vão ao encontro do que o leitor acredita (Shane, 2020).

Quando o usuário das redes sociais está inserido em contexto de polarização política, seu repertório de conversas e conteúdos recebidos fica intimamente ligado às suas próprias convicções. É um estado em que o usuário não quer ser exposto à contrariedade, consumindo e alimentando apenas temáticas alinhadas às suas ideologias.

É importante destacar as bolhas algorítmicas, câmaras de eco (*echo-chambers*)<sup>34</sup>, ou filtros bolha (*filter bubbles*)<sup>35</sup>, que são desenvolvidos nas redes sociais por meio das nossas relações, preferências, curtidas. O conteúdo que chega a um usuário acaba ficando limitado às suas preferências ou influenciando o usuário a fazer escolhas, isso faz com que ele permaneça em uma “bolha” ideológica, um ambiente confortável e seguro, no qual dificilmente encontrará algum atrito, ou modifique seu comportamento a partir de manipulação comportamental (Felipe, 2022).

Outros fatores atribuídos à absorção de notícias falsas podem ser: a) a “ignorância pluralística”, que guarda relação com um cenário manipulador de teoria da conspiração quando não se é capaz de visualizar com clareza o posicionamento das outras pessoas, superestimando certos movimentos com uma magnitude que eles não têm de fato; b) o efeito “terceira pessoa” onde o sujeito só enxerga a vulnerabilidade informativa no outro, mas jamais em si mesmo, e c) a fluência, que é a sensação de facilidade em julgar rapidamente as informações recebidas, tendendo a aceitar como verdadeiras aquelas que soam familiares, por exemplo, no caso das *fake news* que voltam a circular um tempo depois de terem sido desmentidas, o sujeito pode recordar-se da notícia mas não de sua falsidade, e por isso lhe soar familiar, considera o fato como verdadeiro quando o processa rapidamente, (Shane, 2020).

---

<sup>34</sup> “[...] servem para descrever um espaço de mídia vinculado e fechado que tem o potencial de ampliar as mensagens entregues ali e isolá-las das mensagens que as contradizem” (Felipe, 2022).

<sup>35</sup> “[...] à personalização de resultados de motores de busca, como o *Google*, e *feeds* de redes sociais, que estão criando um universo único de informação para cada um de nós baseado em nossos gostos” (Felipe, 2022).

Pennycook e Rand (2019) criaram um teste cognitivo (Cognitive Reflection Test (CRT), ou teste de cognição reflexiva) a partir dos estudos de *Kahneman*. O estudo avaliou se as pessoas tendem a acreditar nas notícias falsas mais rapidamente quando estão alinhadas às suas ideologias, ou seja, se o pensamento crítico prevaleceria sobre a subjetividade. O resultado apontou que a maior parte dos candidatos que acreditaram nas *fake news*, não observaram as questões de forma analítica, implicando na necessidade de reforçar o pensamento crítico para combater da desinformação, uma vez que a vulnerabilidade está mais associada à “preguiça” na busca por fontes confiáveis do que nas reais convicções políticas.

A receptividade de informações falsas está ligada ao estado de vida acelerado, em que as pessoas além de viverem no “automático”, estão permanecendo em ambientes hiperconectados. Pontua-se o desenvolvimento desse estilo de vida a partir das seguintes observações, 1. A rotina torna-se acelerada, e a atenção deve ser filtrada, nem todas as informações processadas serão corretamente processadas; 2. Recorre-se a um estilo de vida hiperconectado, onde é possível viver tudo à distância, conversas, pagamentos, transferências bancárias, compras, relacionamentos afetivos, etc.; 3. A hiperconexão possibilita a coleta de um amplo volume de dados, que serão filtrados e convertidos em conhecimento para as empresas de tecnologia; 4. É atribuído um caráter de confiabilidade às opiniões de familiares e amigos e também aos conteúdos recebidos deles.

O ambiente das redes sociais é um facilitador de propagação de *fake news*, uma vez que as opiniões são compartilhadas por pessoas a quem é dirigido algum tipo de confiança e correspondência ideológica, dificilmente questionando os conteúdos recebidos ou visualizados. O algoritmo da rede social irá direcionar conteúdos que tenham afinidade com as preferências desse usuário ou vai manipulá-lo a modificar seu comportamento, a depender dos interesses envolvidos, o que remete à temática da vigilância algorítmica e direcionamento de conteúdos nas redes sociais.

### 5.3 CAMBRIDGE ANALYTICA – ESPIONAGEM POLÍTICA

A política sempre se molda de acordo com o público e em uma sociedade

hiperconectada, é compreensível que também utilize recursos digitais para conquistar seu eleitorado. O problema surge quando se analisa como tais recursos são aplicados, e para entender como foi possível o direcionamento tão preciso da publicidade política dessa eleição, é necessário analisar sua relação com a vigilância digital.

Em 2023, o caso da eleição de Trump (2016) nos Estados Unidos, ainda é referência como escândalo de manipulação política e desinformação nas redes sociais. A campanha de Trump foi sustentada por técnicas psicométricas aplicadas pela *Cambridge Analytica* junto ao *Facebook* (Empoli, 2020), que possibilitaram um amplo conhecimento de perfil dos eleitores e assim, o direcionamento preciso de conteúdo.

Nas eleições de Trump, a desinformação teve uma dinâmica de direcionamento em moldes persuasivos. Isso foi possível por meio do perfilamento de usuários, identificando perfis. Esses perfis eram identificados por meio de *microtargeting*<sup>36</sup>, identificando quem estaria inclinado para uma ou outra decisão. Essa ferramenta foi eficaz através das redes sociais.

O próprio Donald Trump popularizou o termo *fake news* em uma tentativa de atingir, de depreciar as notícias propagadas nas mídias tradicionais que fossem prejudiciais à sua imagem política. Toda mobilização estremeceu a credibilidade da imprensa e a estratégia política se popularizou (Bernardi, 2020), tendo sido utilizada posteriormente no Brasil.

Em contraposto, o próprio candidato e seus apoiadores foram fortes propagadores dessa chamada *fake news* nas redes sociais. Fato é que Trump se utilizou muito das redes sociais, especialmente do *Twitter* para se comunicar diretamente com seu eleitorado de maneira irrestrita (Bernardi, 2020).

Trump, em meados de 2010, era popular entre negros e latinos em razão do seu programa de TV, “O Aprendiz”, apresentado como um programa inclusivo. E na mesma época, durante o mandato do ex-presidente Barack Obama, deu início à construção do seu modelo de política pautado na desinformação, levantando suspeitas de que Obama poderia não ser americano, o que o deslegitimava a ocupar o cargo de presidente (Empoli, 2020).

---

<sup>36</sup>Microsegmentação utilizada para direcionar conteúdo a um eleitor ou consumidor-alvo (Bernardi, 2020).

Em 2015, Trump promove um discurso em que ofende imigrantes mexicanos, os chamando de estupradores; em um segundo discurso, critica um senador, tido como herói de guerra, John McCain, desqualificando seu título de herói por ter sido capturado; em outro momento, profere falas machistas contra uma jornalista de televisão; imita um repórter portador de deficiência física; apelida outros candidatos de forma infantil, e etc. O que causa espanto é o fato de que ao invés de Trump se desculpar, ele tratou os fatos como *fake news*, embora houvesse provas de suas falas (Empoli, 2020).

Esse tipo de comportamento inicia uma sucessão de liberdades para o discurso de ódio, uma vez que a postura agressiva é normalizada, especialmente nos ambientes digitais, e qualquer opositor, ainda que fosse algum jornalista com credibilidade, seria desmoralizado ao cruzar o caminho do então candidato.

Em 2016, a campanha de Trump contra Hillary Clinton foi dirigida pela *Cambridge Analytica* por meio de dados coletados no *Facebook*. A campanha atuava em duas vertentes, a primeira conquistando eleitores, e a segunda desestimulando os eleitores da oponente com um bombardeio de desinformação totalmente direcionada por meio da *microtargeting* (Empoli, 2020).

A empresa britânica de consultoria política, *Cambridge Analytica*, surgiu em 2012, tendo como acionista majoritário o maior doador da campanha política de Trump, Robert Mercer, que se beneficiou das doações que fez às campanhas políticas que apoiou (Bernardi, 2020), e através da rede social *Facebook*, coletou dados pessoais e sensíveis dos usuários, com a finalidade de manipulação de publicidade eleitoral por meio do direcionamento de conteúdo.

A relação da *Cambridge Analytica* com a vigilância algorítmica retoma a análise sobre os metadados. As pessoas tendem a se despreocuparem com a vigilância digital quando entendem que os detalhes de conteúdo, como as palavras ditas em uma ligação ou e-mail não são tão importantes em um contexto de vigilância em massa, mas em verdade o que importa são outras questões mais abrangentes e que relevam mais sobre comportamentos e seus padrões, sendo capaz de definir o perfil de uma pessoa, essa forma de monitoração é possível por meio dos metadados (Snowden, 2019).

A *Meta* – antigo *Facebook*, é proprietária da rede social *Facebook* - combustível para as estratégias de *marketing* político da *Cambridge Analytica* - e também das plataformas, *Instagram* e *WhatsApp*. Quanto maior a utilização

das redes sociais, maior o fornecimento de dados desses usuários para as plataformas. Quanto mais dados, mais conhecimento, e a persuasão se torna robusta por meio desse conhecimento.

Em 2018, a *Cambridge Analytica*, solicitou em juízo a decretação de falência da empresa, que atuava com processamento de dados por meio de procedimentos com legalidade questionável, por meio da coleta ilícita de dados; *software* de segmentação de perfis; persuasão de eleitores indecisos; disparo de *fake news*, por *microtargeting* (Fornasier; Beck, 2020), em uma interferência direta na democracia e autonomia dos eleitores.

A construção de uma retórica adequada ao público, unida à possibilidade de trazer pessoas que pensam de forma diferente para “o outro lado do jogo”, são técnicas de vigilância algorítmica aplicadas ao cenário político. O caso Trump demonstra perfeitamente como a democracia pode ser extinta, dando lugar à polarização a partir da utilização de direcionamento de conteúdo e persuasão no ambiente digital.

#### 5.4 AS ELEIÇÕES BRASILEIRAS – ASCENSÃO E QUEDA NA ERA DIGITAL

No contexto brasileiro, as eleições de 2018 podem ser comparadas à eleição de Trump em 2016, especialmente quanto à normalização dos discursos de ódio. A desconfiança quanto aos partidos políticos e seus representantes também esteve muito presente nas campanhas políticas do Brasil.

Os debates surgidos nas eleições presidenciais de 2018 foram desencadeados por situações ocorridas em cenários políticos anteriores, quando escândalos de corrupção estiveram em pauta com a investigação Lava Jato<sup>37</sup> (Bernardi, 2020). O cenário investigativo não contribuiu para a imagem do Partido dos Trabalhadores - PT.

As eleições que elegeram Bolsonaro como presidente ocorreram em um contexto de “erros e/ou acertos estratégicos de vários atores” em que “poucos apostavam suas fichas na consolidação e na competitividade” do candidato (Moura; Corbellini, 2019, recurso on-line), em razão de diversos fatores que

---

<sup>37</sup>Investigação sobre “crimes de corrupção cometidos por políticos e empresas que concediam serviços ao Estado, causando uma grande mediação e judicialização política” (BERNARDI, 2020, p. 53).

envolveram a campanha de Bolsonaro, como seus discursos com apologia à tortura e ditadura militar, além de pronunciamentos homofóbicos, machistas e racistas.

As redes sociais deram uma nova dimensão para a política brasileira com:

[...] o crescimento da importância das redes sociais, particularmente a disseminação do Whatsapp como nova plataforma de comunicação, que revoluciona a competição eleitoral e o modo de fazer campanha política no Brasil. Acima de tudo, essa era a eleição dos eleitores indignados e “empoderados” pelo telefone celular (Moura; Corbellini, 2019, recurso on-line).

Com a popularização das plataformas e mídias sociais, a desinformação durante as eleições de 2018 foi muito expressiva e impactou fortemente na quantidade de votos recebida pelo candidato Jair Bolsonaro. A própria postura do candidato que se assemelha à de Trump, com discursos de ódio e sensacionalistas, apoiando o uso de armas, e velados sob questões religiosas e conservadoras, atraiu um grande número de simpatizantes.

A propagação de desinformação na internet se dá por diversos fatores, dentre eles, a sensação de impunidade. Considerando que para o sistema legislativo brasileiro a divulgação de *fake news* ou desinformação não era considerada crime, a menos que se enquadrasse nos delitos de calúnia, difamação e injúria, previstos no Código Penal, ou no crime de racismo, da Lei n.º 7.718 de 1989 (Bernardi, 2020).

As novas tecnologias criaram uma conexão entre políticos e eleitores com uma aproximação possibilitada pelas redes sociais na qual é possível que o candidato trabalhe estrategicamente sua imagem pessoal em sua conta particular (Svensson, 2011, apud Viscardi, 2020). As redes passam claramente a ser utilizadas com uma finalidade política e tanto Trump como Bolsorano, utilizaram fortemente o *Twitter* para se comunicar com os eleitores.

O *Twitter* é uma rede social onde se discute os mais variados temas e a quantidade de caracteres de uma postagem é limitada, o que pode ser muito positivo em uma sociedade que não consegue dedicar uma atenção extensa a um único conteúdo; com mensagens menores a probabilidade do leitor lê-las é maior. Dentre suas funcionalidades e possibilidades de interação, estão:

[...] 1) postar sua própria mensagem na rede (com links, imagens e vídeos); 2) “retuitar” a mensagem de alguém, com ou sem um comentário; 3) responder a um tuíte logo abaixo dele e 4) dar “like” em um tuíte sem necessariamente retuitá-lo ou comentá-lo. Um tuíte retuitado por muitas pessoas e que recebe muitos likes e comentários é um tuíte que “viraliza”. Dentre as implicações da viralização, pode-se destacar a chance de se tornar um assunto de destaque na plataforma, ganhando espaço especial na página, e a transformação de anônimos em “famosos instantâneos” (Viscardi, 2020, p. 1139-1140).

No contexto político, a viralização de conteúdos remete à temática da espetacularização da vida política (Penteado, *et al.*, 2011), na qual os produtores de conteúdo podem causar muito barulho e pouca informação.

Uma mudança legislativa em 2017 (Lei n.º 13.487/17 e Lei n.º 13.488/17) alterou as possibilidades de doações para campanhas eleitorais, mas possibilitou as doações *on-line* que fossem originárias de pessoas físicas. Ficou permitido também, que pessoas físicas impulsionassem conteúdos de páginas políticas (Bernardi, 2020).

O desenvolvimento e acessibilidade das grandes massas às mídias interativas permitiu aos cidadãos um palco para expressar suas opiniões, apoios e insatisfações políticas, colocando uma lente sobre a liberdade de expressão, mas não necessariamente apresentando o espaço digital como democrático. Isso por permitir e possibilitar o espalhamento de desinformação que interferem nos processos eleitorais (Rosa, 2020).

A campanha eleitoral para a presidência em 2018 foi marcada pelas manifestações nas redes sociais, e uma das fontes de propagação da dita desinformação, foi a automação. Informações maliciosas espalhadas por *bots*, contas robôs que interagem de forma autônoma. Contudo é preciso pontuar que contas reais podem espalhar tanta desinformação quanto robôs (Bernardi, 2020).

A postura de Bolsonaro parecia facilitar o trabalho de campanha de seu maior oponente, Fernando Haddad<sup>38</sup>, mas no dia 6 de setembro de 2018, Bolsonaro é vítima de um atentado em que leva uma facada, sendo atingido no

---

<sup>38</sup> Candidato à Presidência da República pelo PT, Partido dos Trabalhadores em 2018.

abdômen (Moura; Corbellini, 2019) e indo direto para o topo da sua carreira política.

Grandes veículos de comunicação como a rede Globo, *The Economist*, *The Guardian*, desqualificavam o Bolsonaro enquanto candidato à presidência e depois de eleito, a estratégia utilizada por ele para se sobressair às críticas da mídia tradicional foi a utilização das mídias digitais. Assim como Trump, Bolsonaro utilizou muito o *Twitter* e o *Facebook* e caracterizava as notícias que o desqualificavam como *fake news* (Bernardi, 2020).

O papel da imprensa foi deslocado para as mídias de comunicação digital, em um espaço onde qualquer pessoa pode participar como noticiante ou espectador. Os usuários da rede promovem conteúdos de forma livre e podem compartilhar informações por meio de aplicativos de mensagens e redes sociais. Com a acessibilidade ao espaço virtual, as pessoas deixam de ser apenas espectadoras e meros receptores de informação, passando a atuar de forma ativa na comunicação (Rais; Sales, 2020).

As eleições de 2018 foram envoltas por escândalos, dentre eles, a suspeita de que empresários teriam patrocinado pacotes de envio de mensagens com desinformação sobre o PT. Em investigação, a Folha de São Paulo “encontrou documentos e áudios que reforçam essa narrativa, inclusive envolvendo a agência espanhola *Enviawhats* como contratada por empresários brasileiros para fazer disparos pró-Bolsonaro” (Bernardi, 2020, p. 57).

O uso intensivo da internet criou um contexto de polarização política, especialmente através do uso de ferramentas de campanha e *marketing* aplicadas às redes sociais e aplicativos de mensagens instantâneas, como *WhatsApp*, (Rosa, 2020).

As eleições de 2018 demonstram a possibilidade de impacto das redes sociais na esfera política e no direcionamento da democracia, a partir da construção de imagens dos atores envolvidos por eles mesmos e por oponentes políticos e até mesmo através da própria população que dispõe de acesso à internet. Bolsonaro construiu uma imagem “politicamente incorreta”, criando um solo fértil para apoiadores que seguiam a mesma linha de pensamentos conservadores ou se encontravam insatisfeitos com o PT (Renno, 2022), e as *fake news* e desinformação foram instrumentos para a construção social política promovida pelo ex-presidente.

A partir do cenário politicamente desgastante, instituído pelo mandato de 4 (quatro) anos de Bolsonaro e a recuperação econômica pós-pandemia, as eleições de 2022 se mostraram como um divisor de águas e também um divisor da população no que se refere aos posicionamentos políticos.

Os discursos continuaram inflamados e com a iminência de perder as eleições de 2022, a direita potencializou a desinformação descredibilizando as urnas eletrônicas e o processo eleitoral, por meio de variadas *fake news* espalhadas sobre o tema (TRE-GO, 2022).

As *fake news* ainda não possuem regulamentação no ordenamento jurídico brasileiro, mas algumas medidas de verificação foram implantadas por meio de sites que informam se determinada notícia é verdadeira ou falsa, contudo dependem que o próprio receptor da notícia tenha disposição de investigar sua veracidade, e considerando o que já foi abordado anteriormente, para receptores que processam informações de forma automática, não se mostra como uma solução eficaz, uma vez que algumas pessoas preferem compartilhar as notícias sem verificar sua veracidade.

Com um resultado acirrado, Lula ganhou as eleições de 2022, destronando o ex-presidente Bolsonaro e mobilizando a insatisfação de seus apoiadores.

Longe de buscar aprofundar o palco político das eleições brasileiras, considerando que a abordagem envolve complexa e ampla temática, como os problemas do contexto pandêmico, agenda ambiental, problemas sociais e econômicos, o que se buscou abordar nesse tópico foram as possibilidades de “ganhar e perder” trazidas pelo ambiente digital. A desinformação e manipulação política é uma via de mão dupla, podendo ser utilizada por vários candidatos como um experimento social digital, em que vencerá as melhores estratégias de *marketing* e contenção de crises.

## 6 TECNOLOGIAS E OBSTÁCULOS À REGULAMENTAÇÃO

A sociedade da informação tem a capacidade de “agir à distância”, não sendo necessário aguardar um encontro ou uma viagem para receber uma resposta que pode vir em alguns minutos ou algumas horas, apesar disso, muitos também vislumbram a distância que existe entre o ato e seu resultado como encorajamento para qualquer ação que não tomariam frente à frente (Bauman; Lyon, 2013), além da sensação de impunidade e anonimato propiciadas pela internet.

A geração da informação foi a primeira a experimentar o ambiente digital em seu formato mais aprimorado, e está relacionada à sociedade de dados, sendo que ambas pertencem a uma nova dinâmica se comparadas à fase anterior à implementação da excessiva coleta e possibilidades de processamento de dados digitais (Florêncio, 2019).

Na dinâmica entre sociedade da informação e sociedade de dados, tem-se a economia da atenção, como uma nova engrenagem da economia, possibilitada pela massiva e constante produção de dados, enquanto consequência da hiperconexão e dispositivos com tecnologias invasivas.

Florêncio (2019) levanta uma reflexão sobre a existência de um “dilema de causalidade” entre dados e tecnologia, em que se confunde qual dos elementos possibilita o outro, se o excesso de tecnologias potencializa a quantidade de dados coletados, ou se o imenso volume de dados impulsiona a criação de novas tecnologias.

Partindo da ideia trabalhada ao longo da pesquisa, as novas tecnologias digitalizaram o “eu” e a vida, refletindo a personalidade humana no ambiente digital. Hoje as pessoas coexistem na vida física e virtual, onde a privacidade e direitos da personalidade ficam ameaçados pelo excesso e risco de exposição.

A internet já está incorporada na sociedade há muitos anos e sua acessibilidade vem crescendo, assim como as facilidades proporcionadas pelas tecnologias. Também cresce o incentivo à utilização das tecnologias e sua inserção nos mais diversos serviços, como para acessibilidade ao setor público (Pinho, 2008).

Não se pretende desacreditar a positividade da inteligência artificial, mas alertar que diante do cenário hiperconectado é preciso repensar o Direito, as

legislações existentes e a eficácia no ambiente da inteligência artificial para alcançar a proteção além dos dados, mas também do sujeito e suas particularidades.

## 6.1 LEGISLAÇÕES BRASILEIRAS NO DIGITAL

A partir da implementação dos meios eletrônicos, foram surgindo legislações pertinentes que regulamentaram as temáticas em voga. O desenvolvimento tecnológico da sociedade está sempre em descompasso com o Direito. Quando visualiza-se os problemas sociais decorrentes das novas inovações, dificilmente o universo jurídico estará antecipado a solucionar, implementando discussões e normativas posteriores.

A doutrina aponta que o Direito Digital seria, na verdade, um “sobredireito”, sobre o qual se visualiza nos dilemas de sua temática, a aplicação de outros instrumentos da esfera jurídica, outras áreas do Direito (Pinheiro, 2021).

Na linha de pesquisa abordada, as legislações pertinentes seguem dois prismas: o da proteção de dados e consequente privacidade e o do direito do consumidor. As inovações tecnológicas foram estudadas a partir de um ponto de vista da comunicação em massa e influência das publicidades, trazendo um entendimento do usuário da internet enquanto consumidor de serviços e produtos ou de informações.

Nessa perspectiva, o traço legislativo brasileiro em direção à proteção da privacidade, conta com a Lei de Interceptação Telefônica – Lei n.º 9.296 de 1996, que regulamentou o previsto no artigo 5º, inciso XII, da Constituição Federal de 1988, quanto à inviolabilidade do sigilo das comunicações telefônicas (Brasil, 1996).

A interceptação telefônica é o “grampo”, quando é possível escutar a conversa de duas ou mais pessoas em uma ligação via telefone (Lopes; Jordace, 2021). Embora não faça muito sentido hoje em dia, quando as comunicações se dão em maior parte por aplicativos de conversa, à época da lei não existiam smartphones e os telefones eram muito utilizados como meio de comunicação via ligação.

A quebra de sigilo de registros telefônicos, por sua vez, refere-se aos dados das ligações efetuadas por determinado usuário da companhia telefônica em seu telefone fixo ou celular pós-pago. A quebra de sigilo também pode recair sobre os dados pessoais do usuário, como endereço e detalhes das chamadas, como horário, valor e duração. Essa modalidade de quebra de sigilo e exposição de dados não estava contemplada na Lei de interceptações e também não dispõe de sigilo absoluto, podendo ser os dados disponibilizados por ordem judicial com finalidade diversa da criminal (Lopes; Jordace, 2021).

No mesmo ano de 1996, é sancionada a Lei de Propriedade Industrial (LPI) - Lei n.º 9.279 de 1996. Já em 1998, surgem as leis n.º 9.609, de Software, e n.º 9.610, de direitos autorais. Essa tríade de leis teve como escopo a proteção de dados, embora não tratassem de dados pessoais (Pinheiro, 2021).

A primeira das sobreditas leis foi de grande importância no marco legal de inovação tecnológica do Brasil, regulando a propriedade industrial por meio da utilização de patentes, marcas, desenhos industriais, indicações geográficas, etc. A segunda e a terceira regularam disciplinas pertinentes à propriedade intelectual, tendo a segunda, a Lei de Software, proteção acerca dos direitos autorais de desenvolvedores de software, e a terceira, direitos autorais sobre as obras criadas (Pinheiro, 2021).

Em 2011, a Lei n.º 12.527, denominada Lei de Acesso à informação, regulamentou a disponibilização de dados públicos, pessoais e/ ou sigilosos pelos três poderes nas esferas federal, estadual e municipal, aos cidadãos (Brasil, 2011).

Pontua-se que a coleta e tratamento de dados podem ocorrer também de forma física. Por exemplo, quando se fala em acesso à informação, não necessariamente serão informações digitais, visto que órgãos públicos possuem grandes acervos físicos, embora em muitos setores, como no judiciário, tem sido implantada a digitalização de documentos físicos. É preciso lembrar que existem os dois aspectos, uma vez que a imersão na sociedade digital faz com que muitas vezes o pensamento relacione de forma automática “tratamento ou coleta de dados” aos dados digitais.

Ainda no ano de 2011, a atriz global Carolina Dieckman, a partir de uma violação de direitos à privacidade, foi chantageada e por não ter cedido à extorsão, sofreu com o vazamento de fotos íntimas. Um apelo e pressão

mediática em torno do tema incentivou, à época, a celeridade do projeto de lei que criminalizou, de forma específica, as condutas ocorridas pertinentes a crimes virtuais e delitos informáticos (Pompeu, 2022).

A partir do caso narrado, é sancionada, em 2012, a Lei n.º 12.737, conhecida por Lei Carolina Dieckmann, que foi um marco legislativo nas matérias de proteção de dados pessoais, introduzindo três tipos penais, relacionados a crimes informáticos, nos artigos 154-A (Invasão de dispositivo informático) e 154-B, no Código Penal (Decreto Lei n.º), e altera os artigos 266, §§1º e 2º e 298, do mesmo dispositivo (Pompeu, 2022).

Voltando ao panorama consumerista, com a mobilidade da internet em alta, as tecnologias mais aprimoradas, e o usuário da internet iniciando uma rotina de maior conexão, no ano de 2013, o Decreto n.º 7.962 regulamentou o comércio eletrônico no Código de Defesa do Consumidor de 1990 (CDC) quanto às disposições de contratações no comércio eletrônico, abordando temáticas sobre as compras *on-line*. O decreto assegurou o direito à informação, o direito ao atendimento facilitado e direito de arrependimento quanto à aquisição do produto no ambiente digital.

Um fator a ser pontuado é que no Código de Defesa do Consumidor (1990), o conceito trazido pelo legislador para “consumidor” é o de “destinatário final” (Brasil, 1990), contudo com o advento das incorporações de tecnologias persuasivas, excesso de coleta de dados e vigilância algorítmica, o consumidor passa a ser visto como o próprio produto (Zuboff, 2020). Porém, as mudanças legislativas consumeristas ainda não acompanharam essa mutação do perfil do consumidor e da confusão tecnológica que recai sobre consumidor e produto.

Acompanhando as modificações sociais e digitais, em 2014, o Brasil teve seu marco normativo no que se refere às leis de internet, com a sanção a Lei n.º 12.965 – Marco Civil da Internet (MCI), que estabeleceu princípios, garantias, direitos e deveres no âmbito do direito digital nacional (Brasil, 2014).

O MCI traz o termo “registros de acesso a aplicações de internet” no seu art. 5º, VIII, como sendo “o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP”, em outras palavras, metadados. O mesmo dispositivo, no seu artigo 7º, VII, regula sobre o não fornecimento desse tipo de metadados a

terceiros, salvo “mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei” (Brasil, 2014, recurso on-line).

O sobredito dispositivo legal traz uma seção sobre proteção dos “registros”, dados pessoais e comunicações privadas, na qual determina que o tratamento dos dados e informações devem “atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas” (Brasil, 2014, recurso on-line) e que os provedores estão obrigados a fornecer dados sob ordem judicial.

Não é possível visualizar nenhum enquadramento legal no MCI para as questões narradas sobre vigilância algorítmica. A proteção de metadados e vedação de compartilhamento com terceiros foram elaboradas de forma tímida, não sendo, aparentemente, capazes de mediar os atuais contornos da vigilância algorítmica. Além disso, a Lei transfere a responsabilidade ao usuário quando prevê liberalidade por meio do instituto do consentimento.

Em 2018, foi elaborado o texto da Lei n.º 13.709, Lei Geral de Proteção de Dados Pessoais (LGPD), que teve seu texto alterado pela Lei n.º 13.853 de 2019 (Brasil, 2018). A Lei Geral de Proteção de Dados não substitui nem revoga o MCI, ela regula o tratamento de dados pessoais - não apenas digitais -, contemplando também bancos de dados físicos; enquanto O MCI é uma lei totalmente voltada para normatizar as relações jurídicas virtuais.

A LGPD traz como conceito de dados pessoais “informação relacionada a pessoa natural identificada ou identificável” (Brasil, 2018, recurso on-line) e ainda que se possa considerar os metadados como elementos capazes de identificar uma pessoa, a Lei não regulamenta o conceito de forma específica.

Ressalta-se que a Lei Geral de Proteção de Dados é um instrumento legislativo muito significativo para o ordenamento jurídico brasileiro, no que diz respeito à implementação de uma cultura digital de privacidade e controle pessoal mais assertivos, no mesmo sentido, o MCI trouxe garantias relevantes aos usuários da internet. Apesar disso, nenhum dos dispositivos abrange regulamentação sobre inteligência artificial ou os limites da vigilância algorítmica, não se apresentando como eficazes neste sentido.

## 6.2 PROTEÇÃO DE DADOS PESSOAIS

O desejo de manter a intimidade, em seus mais diversos sentidos, preservada, de certo sempre existiu. Contudo o direito de exercer tal intimidade surge em 1890, com a publicação de um texto escrito por Warren e Brandeis, intitulado *The right to privacy* ou no português, o direito à privacidade, narrado em uma perspectiva que o definiu como o direito a ser deixado em paz (Rodotà, 2008).

Desde então, vários outros conceitos do direito à privacidade foram levantados e se movimentaram junto com a própria ideia de privacidade, que também se modificava historicamente. Isso, pois o direito à privacidade passou por um longo processo evolutivo que se modificava de acordo com os desdobramentos da sociedade, que influenciavam no conceito de privacidade de cada época.

Ao longo dos anos, a proteção de dados também se tornou importante, ao passo que o conceito de privacidade liga-se ao controle do que se sabe a respeito do indivíduo e como isso poderia ser usado a favor ou contra ele.

O direito de controlar as próprias informações pessoais é o ponto onde surge a confusão de conceitos entre direito à privacidade e direito à proteção de dados. Os direitos à privacidade e à proteção de dados são comumente relacionados, mas é importante diferenciá-los uma vez que são direitos autônomos.

Os atuais contornos da privacidade são formados para além do desejo e direito de estar e ser deixado em paz. A partir da evolução da sociedade e incorporação de novas formas de controle, a privacidade é vista de outra perspectiva como “direito de controle sobre as informações de alguém” e a possibilidade de “determinar como a esfera privada deve ser construída” (Rodotà, 2008, p. 17).

É preciso compreender que o direito à proteção de dados é um dos meios de se alcançar a privacidade, mas não se resume ou se confunde com o conceito de direito à privacidade. Inicialmente, os dois institutos eram amplamente vinculados, mas o direito à proteção de dados “se sofisticou e assumiu características próprias” (Doneda, 2019, p. 24), contemplando garantias além da

privacidade, especialmente adquirindo um caráter protecionista frente ao controle e discriminações que possam atingir direitos fundamentais.

A proteção de dados busca além do direito à privacidade, tutelar outras questões que podem ser as mais variadas, especialmente diante da expansão na utilização do ambiente digital e exponencial crescimento do *Big Data*.

Com o reconhecimento e preocupações advindas do direito digital e a implementação da LGPD no Brasil, o direito à proteção de dados pessoais ganhou status de direito constitucional fundamental autônomo expresso na constituição Federal de 1988, em seu artigo 5º, inciso LXXIX, por meio da Emenda Constitucional n.º 115 de 2022 (Brasil, 1988).

Já o direito à privacidade, por sua vez, consta no artigo 5º, inciso X, do texto constitucional (Brasil, 1988), como proteção à inviolabilidade dos direitos à personalidade, sendo eles o direito à intimidade, à vida privada, à honra e à imagem das pessoas. Assim, a privacidade assume um termo mais amplo, que trata de direitos personalíssimos.

Os dados pessoais determinam os novos contornos sociais, pois consistem nas novas coordenadas de modelagem social. Isso porque extratos do *Big Data* ameaçam tornar-se a base sobre a qual os indivíduos são classificados, avaliados, recompensados ou punidos” (Florêncio, 2019, p. 57), essa segmentação pode ser utilizada a favor ou contra o indivíduo.

Atualmente, “as demandas que agora moldam o perfil da privacidade são de outra ordem, relacionadas à informação pessoal e condicionadas pela tecnologia” (Doneda, 2019, p. 23), contudo é importante ressaltar que a proteção de dados prevista na LGPD, como explanado no tópico anterior, não diz respeito apenas aos dados digitais, sendo necessário, entretanto, considerar que as novas tecnologias trazem o assunto à pauta.

É improvável encontrar hoje uma empresa ou órgão público que esteja 100% (cem por cento) desconectado. Ainda que internamente, haverá sistemas eletrônicos em funcionamento, a utilização de computadores, e outras tecnologias conectadas. Tudo isso deixa os bancos de dados vulneráveis, e é difícil pensar atualmente em proteção de dados sem relacionar os bancos de dados às tecnologias.

Com a ascensão do *Big Data*, a potencialidade das novas tecnologias, e a vigilância algorítmica, os dados pessoais ganharam nova dimensão e

proporção, uma vez que estão disponíveis em um volume exorbitante e são coletados com velocidade, possibilitando maior conhecimento, possibilidade de rastreio e avaliação das pessoas por meio de padrões e contextualização (Florêncio, 2019, p. 58).

Entende-se que, especialmente no ambiente digital, mas não limitado a ele, a proteção de dados pessoais busca preservar a privacidade dos indivíduos de forma ampla, desde questões como o tratamento de dados na utilização de redes sociais e plataformas digitais, até questões explicitamente financeiras, como proteção de dados relacionados à *internet banking*.

O problema dos dados pessoais ocorre no seu tratamento, em outras palavras, como é armazenado e por quanto tempo e com quem são compartilhados. O tratamento deve estar alinhado com parâmetros constitucionais de proteção aos direitos constitucionais fundamentais e possibilidade do usuário das redes sociais de controlar o que é feito com seus dados, vinculando um caráter de veracidade, segurança e “conhecimento da finalidade para a qual serão utilizados” (Doneda, 2019, p. 24).

Apreende-se que o controle que o indivíduo deve ter sobre o tratamento que é aplicado aos seus dados e a finalidade a que se destina a coleta, serve para assegurar e preservar direitos fundamentais como a própria liberdade de expressão. Por exemplo, durante um regime político rígido e conservador, o controle pode implicar em riscos à segurança das pessoas que tenham ideologias diferentes das políticas aplicadas, ou perseguições em razão de discriminações raciais e sexuais, preconceitos de classe, além da própria limitação do direito de se expressar livremente.

O problema do cerceamento de direitos acontece em razão da possibilidade de identificação dos usuários, e ainda há quem acredite no anonimato das redes. Entretanto, a identidade nos ambientes digitais é identificável por meio dos mais diversos dados e metadados fornecidos desde a navegação até na criação de um usuário falso – *fake*.

Constantemente informa-se dados às mais diversas empresas públicas e privadas, além de órgãos governamentais, implicando em um reflexo da personalidade no digital, que merece as mesmas garantias constitucionais que lhe são conferidas no contexto físico. Para alcançar as proteções a personalidade pode-se valer da privacidade como “uma liberdade negativa, que

reconheça e tutele a pessoa contra abusos na obtenção e tratamento destes dados” (Doneda, 2019, p. 23).

Considera-se, também, o direito à proteção de dados para além do “eu”, mas com um olhar de preocupação social, quando o ambiente digital e a coleta massiva de dados a todo momento possibilitam a criação de perfis, que podem ser extremamente prejudiciais às minorias. Os perfis criados também podem tratar de grupos de pessoas, segmentando-as em classes e grupos sociais, tendo implicações e violações sociais, quase sempre com finalidade econômica na qual os filtros servirão para direcionar ou excluir determinado perfil ou grupo de pessoas (Doneda, 2019, p. 24-25).

A proteção de dados como forma de proteção à privacidade, à liberdade de expressão, à segurança, à liberdade de locomoção, etc., ganhou atenção frente aos impactos das plataformas digitais, inteligência artificial e demais serviços que coletam, armazenam dados e tratam dados pessoais com finalidade obscura.

Uma representação da evolução do direito à privacidade e preocupação com proteção de dados foi a comparação de duas falas do criador do *Facebook*, Mark Zuckerberg que, em 2010 disse que privacidade não era algo tão importante já que as pessoas gostam de compartilhar tudo o que fazem, e no ano de 2016, o mesmo empresário disse que o futuro do *Facebook* são contas com mais privacidade (O’Neill, 2019). Para este momento do estudo, pouco importa se as motivações das falas de Zuckerberg foram com finalidade comercial (motivo mais provável), ou se realmente há preocupação com a privacidade dos usuários. O que está por trás desse movimento de opiniões é a didática da privacidade e as preocupações lançadas sobre ela.

Como narrado nos tópicos anteriores, o *Facebook* foi um dos protagonistas de escândalos políticos permitidos por meio de vazamento de dados pessoais de seus usuários, e a partir daí a privacidade e proteção de dados nas redes sociais e plataformas digitais estiveram em pauta. Deve-se então refletir se uma empresa que se preocupa com a privacidade de seus usuários teria fornecido dados como ocorreu.

### 6.3 GOVERNANÇA DOS ALGORITMOS

As análises feitas sobre o Marco Civil da Internet e a Lei Geral de Proteção de Dados, não vislumbraram capacidade legislativa de mitigação dos riscos da vigilância algorítmica e proteção dos metadados sobre a personalidade digital dos seres humanos e seus direitos fundamentais. A IA pode trazer efeitos negativos, o que implica na responsabilidade moral de seus criadores em repensar os processos de seu desenvolvimento.

As inovações tecnológicas carregam consigo efeitos colaterais negativos, não previstos ou pretendidos por seus desenvolvedores, “a fissão nuclear trouxe *Chernobyl* e a ameaça de destruição global; o motor de combustão interna trouxe a poluição do ar, o aquecimento global e a pavimentação do paraíso” (Russel; Norvin, 2013, p. 901). Novas inovações tecnológicas trazem implicações jurídicas e efeitos colaterais diversos.

A inteligência artificial merece destaque nessa discussão, porque trata justamente da tentativa de se criarem mecanismos capazes de “pensar” e agir de forma cada vez mais autônoma. Apesar de o paradigma fundamental do Direito atual ser o antropocentrismo de matriz iluminista, o crescente avanço tecnológico abre a possibilidade para a criação de artefatos mais racionalmente inteligentes que os humanos, o que poderá ser determinante para uma ruptura de paradigma, a partir da qual precisaremos de novas lentes ontológicas e epistemológicas (Magrani; Silva; Viola, 2019, p. 116).

Na inteligência artificial, os algoritmos estão como protagonistas das tomadas de decisões automatizadas, que decidem o curso de vida das pessoas como nas decisões de ordem financeira, saúde, educação, política, oportunidades de emprego, segurança pública e etc. Entre os problemas causados por algoritmos automatizados, estão em destaque as questões relativas à sua opacidade ou falta de transparência e responsabilidade (*accountability*) (Florêncio, 2019).

Os algoritmos de inteligência artificial estão incorporados ao cotidiano e à vida humana trazendo facilidades que não seriam possíveis sem as tecnologias inteligentes. Do outro lado da moeda tem-se os riscos decorrentes da utilização dessas tecnologias, e a governança algorítmica é uma das abordagens

levantadas como solução para os problemas decorrentes das implicações negativas da inteligência artificial, preservando seus benefícios.

Primeiramente, é preciso distinguir a regulação feita por algoritmos, que é quando os algoritmos são aplicados sob pessoas e seus dispositivos inteligentes, e a regulação feita pelo ordenamento jurídico, por meio de instrumentos normativos e legais sobre os algoritmos (Silveira, 2020).

Governança é o ato de governar e guarda relação com organização, liderança, estratégia e controle. A governança algorítmica está amplamente associada à transparência e responsabilidades nos processos automatizados, sendo a opacidade um grande obstáculo à governança (Magrani, 2019).

E no que diz respeito à opacidade:

[...] existem justificativas não técnicas para a sua opacidade. Algumas dessas justificativas se baseiam em questões relativas à concorrência. Um algoritmo aberto pode colocar a empresa por ele responsável em desvantagem diante da concorrência. Outras se baseiam na propriedade intelectual: há países onde a lei protege o sigilo comercial ou a propriedade intelectual das empresas. Outra razão para não se abrir determinados algoritmos é a possibilidade de algumas pessoas, uma vez cientes das suas características, darem um jeito de “enganar” o algoritmo (Gillespie, 2014, apud Doneda; Almeida, 2016, recurso on-line).

A opacidade é a falta de transparência e meios para identificar o resultado que pode ser gerado pelo algoritmo de *machine learning*. A falta de instrumentos e capacidade humana para prever os resultados algorítmicos desaguam em problemas sociais que afetam esferas significativas da vida humana. Em razão disso, o assunto da regulamentação dos algoritmos tem sido levantado como possível solução ou mitigação dos efeitos (Magrani, 2019).

A transparência que se espera dos algoritmos diz respeito às possibilidades humanas de ler, acessar e compreender os códigos de programação. Isso porque a finalidade da utilização de técnicas algorítmicas é agilizar os processos com eficiência, mas quando esses elementos trabalham de forma obscura, sem que se possa compreender seu funcionamento, as implicações podem ser negativas e recair sobre questões sociais pertinentes à segmentação de usuários por meio de *machine learning* (Florêncio, 2019).

As implicações negativas dos algoritmos, como as discriminatórias, não são produzidas de forma intencional pelo programador, mas o caráter de opacidade atribuído as tecnologias inteligentes dificulta a identificação dos mecanismos discriminatórios (Braga, 2019).

A injustiça algorítmica ou discriminação algorítmica representa um risco às igualdades constitucionais, minando para alguns perfis o acesso à determinadas oportunidades, ou colocando uma lente de otimismo sobre uma oportunidade que não é tão boa quanto aparenta ser, induzindo o indivíduo ao erro, trazendo-lhe riscos ou ameaças a direitos personalíssimos (Florêncio, 2019, p. 219).

Os criadores de tecnologias, enquanto cientistas, “programadores e engenheiros podem ter dificuldade em traduzir valores éticos e fundamentais em demandas que afetam decisivamente a vida das pessoas” (Negri, 2020), e os algoritmos trouxeram novas preocupações para o campo da inovação:

- As pessoas poderiam perder seus empregos para a automação.
- As pessoas poderiam ter muito (ou pouco) tempo de lazer.
- As pessoas poderiam perder seu sentido de identidade.
- Sistemas de IA poderiam ser utilizados para fins indesejáveis.
- O uso de sistemas de IA poderia resultar na perda de responsabilidade.
- O sucesso da IA poderia significar o fim da raça humana. (Russel; Norvin, 2013, p. 901).

Quanto aos empregos, atualmente, tem-se uma ideia de que a IA, na verdade, gerou mais empregos do que diminuiu, contudo exige novas qualificações. Diferente do que se pensava inicialmente sobre as máquinas substituírem os seres humanos, a verdade é que foram desenvolvidas para os auxiliar. Em relação ao ritmo das jornadas de trabalho, a IA deixou o cenário da inovação mais competitivo, existindo uma ideia de que seja necessário trabalhar mais, ao passo que também é possível aproveitar das tecnologias autônomas para diminuir por um período, o fluxo de trabalho intenso (Russel; Norvin, 2013).

No que se refere à perda do sentido de identidade, é possível que aconteça a partir da perda da autonomia, que vem sendo ameaçada pela hiperconexão e exposição às tecnologias invasivas. Já as finalidades

indesejáveis estão refletidas no afastamento do ser humano das decisões automatizadas, o que afasta a possibilidade de controle humano sobre as tecnologias, incidindo na violação das liberdades civis (Russel; Norvin, 2013).

A automação, por sua vez, levanta questões sobre quem seria o responsável legal pelas ações dos robôs e “em razão da indefinição da natureza da própria tecnologia em questão, o Direito se vê obrigado a recorrer a velhas figuras, conceitos já conhecidos, que nos auxiliam a nos aproximar” (Negri, 2021, recurso *on-line*) das novas tecnologias. Nas palavras de Castro Júnior (2009, apud Magrani; Silva; Viola, 2019, p. 116) modificações legislativas no ordenamento jurídico brasileiro e de Portugal introduziram um novo conceito de pessoa, excluindo adjetivos e possibilitando que se entenda como detentor da personalidade jurídica “não apenas o Homem, dando chances à teoria do direito animal e, assim, também a do direito robótico para que um robô seja juridicamente qualificado como Pessoa”.

Seguindo na mesma direção, a proposta do Parlamento Europeu, em 2017, para solucionar a problemática de responsabilização civil dos robôs, seria lhes atribuir uma personalidade eletrônica (Negri, 2021). Pontua-se que a personalidade eletrônica abordada neste contexto não guarda relação com a personalidade datificada que foi estudada na pesquisa, uma vez que a personalidade digital (datificada) seria a representação do “eu” humano no ambiente virtual, e a proposta sobre regulamentação dos robôs seria a criação da personalidade eletrônica para uma entidade exclusivamente eletrônica, ainda que possa estar compartilhando o ambiente físico com humanos.

Com a proposta de personalidade eletrônica para robôs, enxerga-se uma confusão quando o instituto da responsabilidade foi atrelado à personalidade. Além disso, a personalidade eletrônica pode não solucionar o problema de responsabilização em tela e ainda repetir padrões que o Direito tem frente à tecnologia ao não individualizar as entidades, desconsiderando os modelos de aplicação de IA em diferentes finalidades (Negri, 2020). É necessário também uma reflexão ética sobre quais responsabilidades devem ser imputadas aos humanos, enquanto responsáveis por sistemas inteligentes, e aos robôs (Magrani; Silva; Viola, 2019).

Sobre a preocupação da IA extinguir a raça humana, considera-se que toda e qualquer tecnologia tem potencialidade danosa, a depender do sujeito

que a manipula. A problemática da inteligência artificial gira em torno dela própria ser o agente potencialmente nocivo a partir da automação por meio da qual a aprendizagem da máquina pode percorrer por caminhos discriminatórios, mas nessa perspectiva de aprendizagem na tomada de decisões “[...] pode-se esperar que um robô que seja inteligente o suficiente para descobrir como terminar com a raça humana também seja inteligente o suficiente para descobrir que não era a função utilidade pretendida” (Russel; Norvin, 2013, p. 903).

Isaac Asimov<sup>39</sup> abordou três leis da robótica que são razoáveis para o ser humano, mas difíceis de aplicar na prática da programação (Russel; Norvin, 2013):

1. Um robô não pode ferir um ser humano ou, por omissão, permitir que um ser humano sofra algum mal.
2. Um robô deve obedecer às ordens que lhe sejam dadas por seres humanos, exceto nos casos em que tais ordens contrariem a primeira lei.
3. Um robô deve proteger sua própria existência desde que tal proteção não entre em conflito com a primeira ou segunda lei (Russel; Norvin, 2013, p. 904-905).

Russel e Norvin (2013) explicam que a dificuldade de aplicação das leis na prática da programação ocorre em razão de serem elas ponderadas uma contra a outra, não sendo lógicas absolutas, em síntese, os autores argumentam que caso fossem trazidas para a realidade fática, poderia ocorrer de uma ação anular a outra.

A partir da ficção de Asimov, Pasquale sugere quatro novas leis destinadas a regular o trabalho dos desenvolvedores de sistemas de IA: 1. Os sistemas robóticos devem auxiliar os profissionais; 2. Os sistemas inteligentes e a IA não devem “falsificar” a humanidade, como nas *deep fakes*<sup>40</sup>; 3. “Não devem intensificar as corridas armamentistas de soma zero”; 4. Informar a identidade dos desenvolvedores (Pasquale, 2020, p. 13, apud Negri, 2021, recurso *on-line*).

A temática e os desdobramentos da inteligência artificial são extremamente extensos, mas considerando a abordagem da pesquisa, analisando os pontos considerados relevantes e sua interconexão, tem-se que

---

<sup>39</sup>Escritor de ficção científica.

<sup>40</sup>Técnica de IA capaz de reproduzir digitalmente a pessoa humana com imagens, como manipular vídeos atribuindo falas falsas à imagem de uma pessoa.

as leis sugeridas por Pasquale<sup>41</sup> (2020, apud Negri, 2021), guardam relação com as pontuações levantadas por Russel e Novin (2013). O ser humano não deve ser substituído pela IA; as personalidades, embora datificadas, não devem ser utilizadas para incorporar avatares no virtual, especialmente com a finalidade de falsificar discursos e comprometer direitos à imagem. É necessário utilizar os sistemas de IA para segurança pública com ética, e é preciso conhecer quem deve ser responsabilizado pela utilização indevida ou antiética das tecnologias.

Observando o cenário tecnodigital, em 2015, a *European Data Protection Supervisor*<sup>42</sup>, autoridade de proteção de dados da União Europeia cria um grupo consultivo externo sobre dimensões éticas e proteção de dados, o *Ethics Advisory Group (EAG)*. Após três anos, em 2018, o EAG emitiu um relatório<sup>43</sup> sobre a nova ética, tendo como fundamentos o direito à privacidade e a proteção de dados pessoais enquanto direitos basilares para a preservação da dignidade da pessoa humana, e dispondo que “ao passo que reconhece a evolução tecnológica, impõe que esta deve ser norteadada por valores humanos, os quais devem permanecer intocados pelas tecnologias” (Florêncio, 2019, p. 217). Atualmente, a Europa já dispõe de normativa direta para a regulamentação da IA, que será abordada no tópico seguinte.

A partir da relação de fundamentação ética sobre proteção de dados, privacidade e dignidade da pessoa humana, rememora-se que os algoritmos, em verdade, não seriam a potência destrutiva que são, se não houvessem dados submetidos ao seu processamento, sendo então o tratamento legal da base de dados um caminho de governança algorítmica externa ao seu próprio sistema (Doneda; Almeida, 2016, recurso on-line).

Driblar a opacidade algorítmica parece ser o maior desafio para alcançar a aplicabilidade da governança por meio da transparência e responsabilidade. Cabe a reflexão se o caminho mais curto para a regulamentação da vigilância algorítmica estaria no desenvolvimento dos sistemas inteligentes ou na utilização de tais sistemas.

---

<sup>41</sup>Professor e autor, especialista em IA.

<sup>42</sup>Autoridade Europeia para a Proteção de Dados.

<sup>43</sup>Foram autores do relatório: “Peter Burgess, Luciano Floridi, Aurélie Pols e Jeroen Van Hoven” (Florêncio, 2019, p. 217).

O capítulo seguinte abordará as perspectivas regulatórias recentes na direção de se estabelecer uma IA mais justa, menos discriminatória e mais controlável, com parâmetros de privacidade e proteção de dados mais bem delineados.

#### 6.4 IA E REGULAÇÃO

A tecnologia amplamente avançada não dispõe de máquinas que sejam em sua totalidade autônomas, sendo necessário o intermédio do ser humano no seu funcionamento. Contudo é possível supor, a partir dos rápidos avanços tecnológicos, que a autonomia das entidades artificiais seja cada vez mais aprimorada, o que levanta questões sobre a responsabilidade e ética dos agentes envolvidos (Magrani; Silva; Viola, 2019).

O uso de algoritmos para regular conjuntos de dados está no cerne da maioria dos arcabouços jurídicos para a proteção dos dados, o que também exige que esses conjuntos de dados sejam legítimos e corretos, cumprindo vários requisitos para atender a esses critérios. Um bom exemplo seria o consentimento para o uso de dados pessoais em várias ocasiões, uma vez que a propriedade é outra das questões que assomam, e identificar conjuntos de dados específicos – de maneira a permitir consentimento para tratamento e uso de dados, seja para uso pessoal ou simplesmente originado por um cidadão – também deveria ser assunto para regulação (Doneda; Almeida, 2016, recurso on-line).

O consentimento é, por vezes, abordado como uma robusta solução jurídica às demandas decorrentes das aplicações algorítmicas sobre os usuários da rede, contudo esse instrumento jurídico carrega um peso de responsabilização do usuário enquanto parte vulnerável da relação entre pessoa x algoritmo x empresa/ governo, na qual com frequência não se tem a prevalência da autodeterminação informativa. Os desdobramentos sobre o consentimento serão abordados no tópico seguinte.

Para que o consentimento seja eficaz, é preciso que a utilização dos sistemas inteligentes e respectivos bancos de dados sejam explicados de forma inteligível (Florêncio, 2019). Do contrário, quando a opacidade implica no desconhecimento do próprio desenvolvedor do produto, não há que se falar em

validade do consentimento, uma vez que ninguém detinha verdadeiro conhecimento acerca da finalidade.

A opacidade algorítmica prejudica o consentimento quando impede que o usuário da tecnologia desconheça seu real funcionamento. Conforme já mencionado no tópico anterior, muitas vezes a opacidade está relacionada com segredos do negócio, com a finalidade de manter vantagem competitiva sobre outras empresas, preservando seu direito de livre iniciativa de mercado e utilizando do segredo industrial, resultando no desinteresse do proprietário do código em explicar seu real funcionamento (Florêncio, 2019).

Frank Pasquale, pontua três formas estratégicas de sigilo (opacidade): sigilo real, sigilo legal e ofuscação:

Por **sigilo real** pode ser entendida a situação que estabelece uma barreira entre o conteúdo escondido e o acesso não autorizado a esse conteúdo. Um exemplo desse caso é o e-mail que protegemos com uma senha. O **sigilo legal**, por sua vez, obriga que determinados dados e informações mantenham seu conteúdo sigiloso, a exemplo de um empregado de banco que é obrigado seja por força de lei, seja por força do contrato de trabalho, a não revelar o saldo de seus clientes a terceiros. Já a **ofuscação** guarda relação com atos deliberados de ocultação quando o sigilo não pode ser alegado na situação. Como exemplo, cite-se uma empresa que, em resposta a um pedido de informações, entrega milhares de páginas de documentos, forçando o interessado a perder tempo, como a tarefa de procurar uma agulha no palheiro (Pasquale, 2015, apud Florêncio, 2019, p. 227) (Grifos meus).

A solução não está na exposição do segredo industrial das empresas que deve permanecer preservado, contudo sem construir pontes inalcançáveis para a transparência. O tratamento de dados é diferente do funcionamento dos algoritmos. O algoritmo funciona em três camadas interconectadas, 1. Entrada de dados brutos, guarda relação com a autodeterminação informacional; 2. Opacidade – operações aplicadas sobre os dados; 3. Saída – resultado dos dados após as operações, que pode conter dados que não foram inseridos na primeira etapa, mas adquiridos após o tratamento. Para a validade do consentimento, seria necessário que o titular dos dados compreendesse o processo das três camadas (Florêncio, 2019).

Outra questão a ser pontuada acerca do consentimento são as formas como as informações podem ser transmitidas aos usuários. Como abordado anteriormente, os usuários da internet são inquietos, incapazes, em sua maioria, de absorver informações de forma completa ou checar as fontes (Shane, 2020).

O mesmo perfil do usuário que não checa a veracidade das informações recebidas, certamente será aplicado para o conhecimento técnico das informações pertinentes ao tratamento dos seus dados. Diariamente termos e contratos são assinados sem prévio conhecimento, apenas para se ter acesso à determinado serviço ou funcionalidade:

Consentimento vem de *co-sentire*. Existe um envolvimento para conhecer e concordar com as bases as quais se consente. Porém, na toada da vida de hoje, de imediatismo e tempo escasso, parece não haver espaço para querer saber mais sobre as bases as quais se confere a concordância. As pessoas são rápidas, estão com pressa e sem paciência. Nesse contexto, há aqueles que pregam a morte das políticas de privacidade (de sites e aplicativos), pois entendem que de nada servem, uma vez que praticamente ninguém as lê (Florêncio, 2019, p. 264).

As pessoas não dispõem de tempo e interesse para fazer leituras, compreender termos, e parecem não ter muito interesse em relação ao tratamento de dados, sendo questionável as circunstâncias do consentimento.

Hoje, não se reconhece o instituto da IA como uma pessoa, ou seja, um sujeito de direitos, não podendo a entidade eletrônica ser responsabilizada pelas consequências de sua aplicabilidade, motivo pelo qual, parte da doutrina compreende que a responsabilidade deve ser imputada à “pessoa (natural ou uma entidade) em nome de quem um programa foi criado” (Magrani; Silva; Viola, 2019, p. 117).

A regulamentação das temáticas de proteção de dados no ambiente digital foi iniciada por leis não estatais, como códigos de autorregulamentação promovidos por entidades privadas desenvolvedoras de sistemas inteligentes; depois por regramentos éticos estabelecidos por entidades como a Organização para a Cooperação e Desenvolvimento Econômico ou Económico (OCDE) e a Unesco; e depois por indústrias privadas. Ocorre que este tipo de regulamentação não dispõe de vinculação legislativa, não obrigando as empresas ou órgãos públicos a submeter-se a elas (Marques; Baquero, 2023).

Voltando às regulamentações, em abril de 2021, na corrida pela regulamentação da Inteligência Artificial, a Comissão Europeia apresentou uma proposta para regulamentar a tecnologia no âmbito de seu desenvolvimento, comercialização e aplicação da IA (Negri, 2021). No dia 14 de junho de 2023, membros do parlamento Europeu votaram e aprovaram a lei, em Estrasburgo, na França (ABCD USP, 2023).

A lei europeia sobre IA reforça critérios de privacidade e transparência, sendo o primeiro regulamento do tipo, caminhando para uma prevenção parcial das implicações negativas da vigilância algorítmica por meio das categorias de risco trazidas no documento, sendo três:

**Em primeiro lugar**, aplicativos e sistemas que criam um risco inaceitável, como pontuação social administrada pelo governo do tipo usado na China, são banidos. **Em segundo lugar**, os aplicativos de alto risco, como uma ferramenta de digitalização de currículos que classifica os candidatos a empregos, estão sujeitos a requisitos legais específicos. **Por fim**, aplicativos não explicitamente banidos ou listados como de alto risco são deixados sem regulamentação (ABCD USP, 2023), (Grifos meus).

A proposta europeia de regulamentação da IA afastou as questões de atribuição de personalidade jurídica eletrônica aos sistemas e robôs inteligentes, baseando a normativa nas categorias de riscos expostas. Pode-se considerar a categorização como o reconhecimento de que “os riscos associados aos usos de novas tecnologias podem não se distribuir de forma linear entre pessoas e grupos” (Negri, 2021, recurso *on-line*), isso em razão de algumas segmentações de perfis individuais ou grupos, representarem um efeito negativo mais expressivo em relação a outros.

Se a aplicação da lei for eficiente, muitos problemas decorrentes da mineração de dados podem ser mitigados, enfrentando uma rigidez maior na sua aplicação. Contudo vários especialistas da área do direito digital e ciências sociais analisaram a regulamentação europeia de inteligência artificial com ressalvas, identificando críticas ao modelo legislativo, como a possibilidade de algumas atividades ficarem sem regulamentação por não se enquadrarem de forma explícita nos requisitos; as lacunas; inflexibilidade, e exceções trazidas pelo dispositivo, que podem ter impacto social para as minorias (AI ACT, 2023).

No Brasil, o Projeto de Lei (PL) n.º 21 de 2020, de iniciativa do Deputado Federal, Eduardo Bismark (PDT-CE), buscou a regulamentação da IA no país, estabelecendo como critérios basilares, transparência, direitos humanos e valores democráticos, além da preservação de direito à igualdade, a não discriminação, a pluralidade, a livre iniciativa e a proteção dos dados (Doederlein, 2020).

A partir do PL 21/2020, as discussões sobre o tema se solidificaram, e em 2022, a criação de um dispositivo legal passou a ser discutida no Senado brasileiro, com a instituição de uma comissão de juristas (CJSUBIA) que foi responsável por analisar os projetos de lei “(PLs) 5.051/2019, de autoria do Senador Styvenson Valentim (Podemos-RN); 21/2020, do Deputado Eduardo Bismarck (PDT-CE); e 872/2021, do Senador Veneziano Vital do Rêgo (MDB-PB)” criando um documento substitutivo, PL n.º 2338 de 2023 (Gov, 2023, recurso on-line).

O novo PL segue a linha da proposta da União Europeia (AI Act) para regulação do tema, ao prever o detalhamento de obrigações e responsabilidades aos fornecedores e operadores de IA no próprio texto da lei, o que difere completamente da abordagem principiológica do PL 21/20, oriundo da Câmara dos Deputados, e da ênfase na regulação setorial e forte investimento privado, dos EUA (Blum, 2023).

O PL n.º 2338 de 2023 traz alguns conceitos acerca da operação de sistemas de IA como: 1. Fornecedor é o desenvolvedor, podendo ser pessoa física ou jurídica; 2. Operador, usuário da tecnologia com finalidade profissional, podendo ser pessoa física ou jurídica; 3. Agentes de IA, fornecedores e operadores de IA; e 4. Autoridade competente, órgão ou entidade fiscalizador da administração pública federal (Blum, 2023).

Há no dispositivo brasileiro a avaliação preliminar e classificação de risco (excessivo, alto), há determinação de governança voltada à transparência, mitigação de vieses discriminatórios, conformidade com a LGPD, medidas de segurança da informação, dentre outros. Sendo que para os sistemas de IA de alto risco tem-se ainda, a previsão de supervisão humana para corrigir decisões e avaliação de impacto algorítmico e garantia da preservação do segredo industrial e comercial (Blum, 2023).

O dispositivo legal traz também como instrumento legal, a comunicação de incidentes e a responsabilização Civil para os agentes que causarem danos patrimoniais ou extrapatrimoniais. Sendo que na IA de alto risco, aplica-se a inversão do ônus da prova: o fornecedor ou operador têm responsabilidade objetiva, de acordo com sua participação nos danos. Quanto às sanções, a multa segue o padrão da LGPD, sendo 2% do faturamento, mas com limite de R\$50.000.000,00 (cinquenta milhões) por infração, dentre outras como restrição a determinados bancos de dados (Blum, 2020).

Para os usuários das tecnologias inteligentes o PL prevê:

(i) o direito à explicação sobre o funcionamento dos sistemas de Inteligência Artificial, (ii) o direito à informação prévia sobre a utilização de IA em um determinado produto ou serviço, (iii) o direito à contestação das decisões e previsões de IA que afetem os interesses de usuários, entre outros (Blum, 2023, recurso on-line).

O Código de Defesa do Consumidor de 1990, em seu artigo 43, garante o acesso às informações pessoais e de consumo, presentes em banco de dados e a conhecimento das fontes originárias dos dados (Brasil, 1990), mas cabe a reflexão se o marco legislativo brasileiro de regulamentação à IA manteve a problemática abordada sobre consentimento, quando não se é possível obter informações claras quanto ao funcionamento dos sistemas inteligentes. Na mesma linha, encontra-se o direito de explicação das decisões automatizadas, pois se as três camadas do tratamento de dados forem consideradas, quando a ocorrência se der em *machine learning*, a camada da opacidade poderá ganhar uma lente de aumento, consequentemente, o mesmo problema afeta os pedidos de revisão das decisões se elas forem revistas por sistemas automatizados de aprendizagem de máquina.

## 7 CONSIDERAÇÕES FINAIS

É possível compreender os moldes atuais das tecnologias como a construção de um modelo econômico e comercial pautado nas comunicações em massa. Com o surgimento da informática e posteriormente, da incorporação da internet como meio de comunicação em massa, a arquitetura das redes proporcionaram uma vigilância constante dos usuários que se mantêm permanentemente conectados.

As tecnologias da comunicação conduziram padrões de publicidade com finalidade econômica e política, contudo esses padrões invadem esferas da privacidade que deslocam o usuário titular de dados de uma situação de controle de dados para uma posição que o submete às manipulações ocasionadas pelo seu fornecimento excessivo de dados. O novo modelo de consumo contempla usuários de internet hiperconectados com acesso constante à informação e possibilidade de comunicação permanente. Com tantas pessoas conectadas ao mesmo tempo, muitos dados são gerados, representando um grande banco de dados brutos coletados.

O excesso de dados coletados precisa de um tratamento específico para que se obtenha informações e conhecimento, uma espécie de filtragem do essencial. Quando os dados brutos são ressignificados em conhecimento, tem-se a datificação da personalidade, uma espécie de virtualização do “eu”, onde é possível construir um perfil do usuário, conhecendo sua personalidade a fundo, a partir de dados e rastros digitais deixados ao longo das conexões.

A mobilidade da internet potencializou a arquitetura de vigilância constante, quando os usuários tiveram a possibilidade de carregar seus dispositivos móveis por toda parte, sempre conectados e acessíveis, iniciaram uma rede de dados pessoais e rastros digitais. Somado a isso, surgem as mídias sociais, ampliando as lentes da hiperconectividade.

As tecnologias dos dispositivos, assim como as tecnologias da rede de conexões ganharam aprimoramento e sofisticação, surgem então aparelhos mais inteligentes e conexões de internet mais rápidas e estáveis. Toda sofisticação dos equipamentos passa a incorporar a rotina dos usuários da internet e até mesmo sua indumentária, por meio de dispositivos inteligentes e *weareables*, traduzindo uma conexão ubíqua, assim como a produção constante

de dados, configurando as possibilidades de se construir a personalidade datificada por meio da vigilância constante a qual os usuários de tecnologias inteligentes se expõem ou são expostos.

Não se pretendeu, com essa pesquisa, aprofundar termos técnicos pertinentes à ciência da computação ou de dados, mas analisar a implicação de algum desses elementos nas relações jurídicas submetidas à vigilância algorítmica, e para isso foi necessário compreender alguns conceitos, ainda que não profundamente, como, algoritmos, inteligência artificial, *machine learning*, e mineração de dados.

A datificação da personalidade é, então, uma consequência da vigilância algorítmica. Algoritmos são códigos matemáticos que dão instruções aos computadores, de simples às mais complexas. Com o desenvolvimento das tecnologias, os algoritmos se sofisticaram e passaram a dispor do que se conhece por inteligência artificial, os algoritmos inteligentes.

As questões jurídicas implicadas pelos algoritmos surgem em sua programação, no que é conhecido como injustiça algorítmica. Ocorre que os algoritmos são códigos criados por humanos, que podem adquirir capacidades sobre-humanas, mas quando são programados recebem vieses (*bias*) de seus programados, que refletem suas percepções boas e ruins, junto a isso, são inseridas questões discriminatórias que podem versar sobre temáticas racistas, machistas e socioeconômicas.

A inteligência artificial é a capacidade dos algoritmos de aprender o que os humanos podem fazer, já na aprendizagem de máquina ou *machine learning*, que é um subcampo da IA, esses códigos conseguem aprender sozinhos, por meio da repetição de atividades, entre erros e acertos.

Na mineração de dados, os algoritmos atuam de forma altamente eficaz, podendo utilizar da aprendizagem de máquina para trabalhar identificando padrões e correlacionando dados, sendo uma técnica extremamente avançada e útil para analisar e processar grandes bancos de dados, que necessitam de capacidade sobre-humana para identificar informações e conhecimento a partir de uma vasta quantidade de dados, em que nem todos serão relevantes.

A partir dos padrões criados tem-se a técnica de *profiling*, que se refere a criação de um perfil de determinado usuário a partir dos seus padrões de utilização da rede.

Um elemento por muito tempo subvalorizado e desconhecido pelos usuários da internet, que possibilita a eficiência da vigilância algorítmica de forma ampla, é o metadado, que pode ser compreendido como “dados sobre os dados”. Os metadados carregam informações que podem ser comprometedoras quanto à privacidade e merecem atenção legislativa por seu caráter invasivo.

As implicações que recaem sobre a personalidade datificada por meio da vigilância algorítmica implicam em pontos relevantes sobre a proteção da pessoa humana, sua privacidade, autonomia, liberdade e escolhas individuais. Com o conhecimento aprofundado dos usuários da rede, a possibilidade de segmentá-los em grupos, influenciar suas escolhas, e manipular comportamentos, influi na manutenção e desenvolvimento das democracias.

O texto aborda a coleta e tratamento de dados como finalidade comercial e econômica, mas os interesses podem ser traduzidos em políticos ao se considerar que as empresas de tecnologias que têm a possibilidade de monetizar os dados de seus usuários por meio da venda dessas informações, podem perfeitamente comercializá-los para entidades ou pessoas com interesse político.

O escândalo da *Cambridge Analytica* e os constantes casos políticos envolvendo *fake news* demonstram a má utilização dos dados coletados em desfavor do seu titular, indivíduo sobre o qual são aplicadas técnicas de análise e persuasão comportamental com finalidade política.

As tecnologias de persuasão e interferências comportamentais devem ser analisadas a partir de uma perspectiva protecionista das liberdades individuais, proteção de dados e privacidade, que busque a preservação dos direitos personalíssimos dos usuários da internet.

Lança-se um olhar sobre as legislações brasileiras de proteção dos usuários no ambiente digital como o Marco Civil da Internet, e legislações de proteção de dados pessoais frente à inteligência artificial. Analisa-se a programação de algoritmos e sistemas inteligentes a partir da observação de um código de ética voltado à robótica e posteriormente, levantado em outros aspectos na regulamentação europeia, buscando afastar repercussões discriminatórias.

O consentimento e direito à explicação, previstos pela LGPD e na proposta legislativa brasileira de regulamentação à IA, também são abordados e

têm sua eficácia questionada no que se refere ao controle dos usuários sobre o tratamento de seus dados e metadados em relação ao seu caráter informacional.

Compreende-se os institutos jurídicos analisados ineficazes na proteção da datificação da personalidade frente à vigilância algorítmica, e visualiza-se como possível recurso, a responsabilização dos desenvolvedores de sistemas e/ou das empresas que contrataram seu desenvolvimento. Contudo ainda que se compreenda a possibilidade de mitigação dos riscos frente ao receio por parte dos desenvolvedores de sofrerem as penalidades, não se trata de uma medida eficaz em sua completude, pelo fato dessa aplicação não ocorrer de forma preventiva contra os efeitos negativos, podendo ser aplicada apenas após o dano ou na comprovação de sua iminência. Ressalta-se ainda, o fator de obscuridade dos algoritmos que muitas vezes irá camuflar os efeitos, dessa forma, compreende-se que os maiores danos podem ocorrer de forma oculta e indireta, não havendo meios da parte interessada tomar conhecimento e buscar a devida reparação.

Volta-se então às hipóteses levantadas inicialmente de que ou “i) *existiriam pontos cegos legislativos sobre a regulamentação dos algoritmos nas questões de vigilância*; ou na possibilidade de existência normativa, ii) *haveria dificuldades de aplicação e fiscalização normativas*”, e na busca pelas respostas foi possível concluir que a primeira hipótese foi confirmada, uma vez que ainda não existe no Brasil, dispositivo vigente para regulamentação de sistemas inteligentes, contudo pontua-se que encontra-se em andamento no Senado Federal, um projeto de lei caminhando para regular a temática.

A segunda hipótese não pode ser confirmada por estar condicionada à negativa da primeira, em outras palavras, frente a ausência de dispositivo legal, não há que se falar sobre eficiência legislativa. Apesar disso, considerando uma análise sobre o PL n.º 2238/23, acredita-se que existirão dificuldades de implementação na aplicação, podendo se originar das lacunas legislativas e tendo como agravante a incultura algorítmica, no sentido do desinteresse dos usuários de tecnologias em preservar seus direitos.

Diante do exposto, fica caracterizada a necessidade de uma releitura mais robusta do direito digital a partir da vigilância algorítmica, uma vez que no modelo de sociedade vivenciado não é possível pensar no afastamento da personalidade datificada. Porém, ainda é possível repensar instrumentos

jurídicos que possam protegê-la de forma individual, quanto aos direitos personalíssimos, ou de forma coletiva, quanto às democracias.

## REFERÊNCIAS

- ABCD USP. Parlamento Europeu vota lei de regulamentação de IA. **ABCD USP**. São Paulo, 2023. Disponível em: <https://www.abcd.usp.br/noticias/parlamento-europeu-regulamentacao-de-ia/>. Acesso em: 5 set. 2023.
- AI ACT, The. The Artificial Intelligence Act. **The AI Act**. 2023. Disponível em: <https://artificialintelligenceact.eu/>. Acesso em: 10 set. 2023.
- BAPTISTA, Erica Anita; ROSSINI, Patrícia; OLIVEIRA, Vanessa Veiga de; STROMER-GALLEY, Jennifer. A circulação da (des)informação política no WhatsApp e no Facebook. **Lumina**, [S. l.], v. 13, n. 3, p. 29–46, 2019. DOI: 10.34019/1981-4070.2019.v13.28667. Disponível em: <https://periodicos.ufjf.br/index.php/lumina/article/view/28667>. Acesso em: 10 set. 2023.
- BAUMAN, Zigmunt. **Vida para o consumo**: a transformação das pessoas em mercadoria. Rio de Janeiro: Zahar, 2008.
- \_\_\_\_\_; Lyon, David. **Vigilância Líquida**. Rio de Janeiro: Zahar, 2013.
- BENTES, Anna. Quase um tique: economia da atenção, vigilância e espetáculo a partir do instagram. **Media Lab UFRJ**, Rio de Janeiro, 19 jun. 2018. Disponível em: <https://medialabufrj.net/projetos/quase-um-tique-economia-da-atencao-vigilancia-e-espetaculo-a-partir-do-instagram/>. Acesso em: mai. 2021.
- BERNARDI, Ana Júlia Bonzanini. **Fake News e as eleições de 2018 no Brasil**: como diminuir a desinformação. 1 ed. Curitiba: 2020.
- BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. 3 ed. Rio de Janeiro: Forense, 2021.
- BLUM, Bruno Ópice. Marco Legal Da Inteligência Artificial No Brasil (PL 2338/2023). **Ópice Blum**. São Paulo, 5 mai. 2023. Disponível em: <https://opiceblum.com.br/marco-legal-da-inteligencia-artificial-no-brasil-pl-2338-2023/>. Acesso em: 09 set. 2023.
- BRAGA, Carolina. Discriminação nas decisões por algoritmos: polícia preditiva. In: FRAZÃO, Ana; MULHOLLAND, Caitlin de (coord.). **Inteligência artificial e direito**: ética, regulação e responsabilidade. São Paulo: Thomson Reuters Brasil, 2019, p. 671-695.
- BRAMAN, Sandra. Tactical memory: the politics of openness in the construction of memory. **First Monday**, v. 11, n. 7, Chicago, 2006. Disponível em: <http://uncommonculture.org/ojs/index.php/fm/article/view/1363/1282>. Acesso em: 10 mai. 2021.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [1988]. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/constituicao/constituicao.htm](http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm). Acesso em: 01 mai. 2021.

\_\_\_\_\_. **Lei n.º 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF: Presidência da República, [1990]. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/leis/l8078compilado.htm](https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm). Acesso em: 01 mai. 2021.

\_\_\_\_\_. **Lei n.º 9.296, de 24 de julho de 1996**. Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal Brasília, DF: Presidência da República, [1996]. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/leis/l9296.htm](https://www.planalto.gov.br/ccivil_03/leis/l9296.htm). Acesso em: 01 mai. 2021.

\_\_\_\_\_. **Lei n.º 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Brasília, DF: Presidência da República, [2002]. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/leis/2002/l10406compilada.htm](https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm). Acesso em: 01 mai. 2021.

\_\_\_\_\_. **Lei n.º 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei n.º 8.112, de 11 de dezembro de 1990; revoga a Lei n.º 11.111, de 5 de maio de 2005, e dispositivos da Lei n.º 8.159, de 8 de janeiro de 1991; e dá outras providências. Brasília, DF: Presidência da República, [2011]. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2011/lei/l12527.htm](https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm). Acesso em: 10 mai. 2021.

\_\_\_\_\_. **Lei n.º 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, [2014]. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2014/lei/l12965.htm](https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm). Acesso em: 10 mai. 2021.

\_\_\_\_\_. **Lei n.º 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2018]. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm). Acesso em: 10 mai. 2021.

\_\_\_\_\_. **Tribunal Superior Eleitoral**. Resolução n.º 23.732 de 2024. Rel. Min. Carmén Lúcia, publicada no Diário de Justiça em 27 fev. 2024. Disponível em: <https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-732-de-27-de-fevereiro-de-2024>. Acesso em: 4 mar. 2024.

COELHO, Taysa. Pager fez sucesso nos anos 1990: relembre o antecessor do SMS e Whatsapp. **Tech Tudo**. 16 dez. 2018. Disponível em: <https://www.techtudo.com.br/noticias/2018/12/pager-fez-sucesso-nos-anos-1990-relembre-o-antecessor-do-sms-e-whatsapp.ghtml>. Acesso em: 30 ago. 2023.

COSTA, Roberto Renato Strauhs da; PENDIUK, Fábio. Direito digital: o marco civil brasileiro da internet e as Inovações jurídicas no ciberespaço. **FESPRR Publica**. Curitiba, v. 2, n. 1. 2018.

DEVINCENZI, Sam. **O uso de tecnologias persuasivas ubíquas para potencializar o processo de aprendizagem baseado em problemas**. 2019. Tese (doutorado) – Programa de Pós-Graduação em Educação em Ciências: Química da Vida e Saúde, Universidade Federal do Rio Grande – FURG. Rio Grande/RS, 2019. Disponível em: <https://repositorio.furg.br/bitstream/handle/1/8854/0000012967.pdf?sequence=1&isAllowed=y>. Acesso em: 31 ago. 2021.

DIJCK, José. Confiarmos nos dados? As implicações da datificação para o monitoramento social. **Matrizes**. São Paulo, v. 11, n. 1, jan./ abr, 2017, p. 39-59. Disponível em: <https://www.revistas.usp.br/matrizes/article/view/131620/127911>. Acesso em: 05 set. 2023.

DOEDERLEIN, Natalia. Projeto cria marco legal para uso de inteligência artificial no Brasil. **Câmera**. Brasília, 4 mar. 2023. Disponível em: <https://www.camara.leg.br/noticias/641927-projeto-cria-marco-legal-para-uso-de-inteligencia-artificial-no-brasil/>. Acesso em: 9 set. 2023.

DOMINGOS, Pedro. **O algoritmo mestre**: como a busca pelo algoritmo de machine learning definitivo recriará nosso mundo. 1ª ed. São Paulo: Novatec, 2017.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: fundamentos da lei geral de proteção de dados. 2 ed. São Paulo: Thomson Reuters Brasil, 2019.

DONEDA, Danilo. ALMEIDA, Virgílio A. F.. O que é a governança de algoritmos?. **Politics**. Rio de Janeiro, out. 2016. Disponível em: <https://politics.org.br/edicoes/o-que-%C3%A9-governan%C3%A7a-de-algoritmos>. Acesso em: 10 set. 2023.

ECO, Humberto. **Como se faz uma tese**. 27 ed. São Paulo: Perspectiva, 2019.

EMPOLI, Giuliano da. **Os engenheiros do Caos**: como as fake News, as teorias da conspiração e os algoritmos estão sendo utilizados para disseminar ódio e medo e influenciar eleições. 1 ed. São Paulo: Vestígio, 2020.

SPADONI, Pedro. Julgamento de processo antitruste contra o Google tem data marcada. **Olhar Digital**, fev. 2024. Disponível em: <https://olhardigital.com.br/2024/02/06/pro/julgamento-de-processo-antitruste-contra-o-google-tem-data-marcada/>. Acesso em: 20 fev. 2024.

FELIPE, Mathias. Câmaras de eco, filtro bolha e polarização: do que estamos falando?. **Desinformante**. 10 fev. 2022. Disponível em:

<https://desinformante.com.br/camaras-de-eco-filtro-bolha-e-polarizacao-do-que-estamos-falando-e-como-se-relacionam/>. Acesso em: 01 mai. 2021.

FIGUEIREDO, Jorge. Internet nas redes móveis: evolução ao longo dos anos e o futuro. **Serviço em Destaque**. Jan. 2023. Disponível em: <https://www.servicoemdestaque.com.br/redes-moveis/#:~:text=Redes%20m%C3%B3veis%20G&text=Esta%20rede%20com e%C3%A7ou%20a%20existir,classificado%20como%20tecnologia%20%2C7 G>. Acesso em: 30 de ago. 2023.

FLORÊNCIO, Juliana Abrúcio. **Proteção de dados na cultura do algoritmo**. 2019. Tese (Doutorado) – Programa de Estudos Pós-Graduados em Direito, Pontifícia Universidade Católica de São Paulo, São Paulo, 2019.

FORNASIER, Mateus de Oliveira; BECK, Cesar. Cambridge Analytica: Escândalo, Legado e Possíveis Futuros para a Democracia. **Revista Direito em Debate**, Ijuí, v. 29, n. 53, p. 182–195, 2020. DOI: 10.21527/2176-6622.2020.53.182-195. Disponível em: <https://www.revistas.unijui.edu.br/index.php/revistadireitoemdebate/article/view/10033>. Acesso em: 01 set. 2023.

GALVÃO, Noemi Dreyer; MARIN, Heimar de Fátima. (2009). Técnica de mineração de dados: uma revisão da literatura. **Acta Paulista De Enfermagem**, Cuiabá, v. 22, n. 5, 686–690, 2009. Disponível em: <https://doi.org/10.1590/S0103-21002009000500014>. Acesso em: 06 set. 2023.

GOOGLE CLOUD. **O que é análise preditiva?**. Disponível em: [https://cloud.google.com/learn/what-is-predictive-analytics?hl=pt-br#:~:text=A%20an%C3%A1lise%20preditiva%20%C3%A9%20o,que%20poss am%20prever%20comportamentos%20futuros.&as\\_qdr=y15](https://cloud.google.com/learn/what-is-predictive-analytics?hl=pt-br#:~:text=A%20an%C3%A1lise%20preditiva%20%C3%A9%20o,que%20poss am%20prever%20comportamentos%20futuros.&as_qdr=y15). Acesso em: 03 set. 2023.

GOV. ANPD publica análise preliminar do Projeto de Lei n.º 2338/2023, que dispõe sobre o uso da Inteligência Artificial. **GOV**. Brasília: 6 jul. 2023. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-analise-preliminar-do-projeto-de-lei-no-2338-2023-que-dispoe-sobre-o-uso-da-inteligencia-artificial>. Acesso em: 09 set. 2023.

HARARI, Yuval. **Homo Deus: uma breve história do amanhã**. 1ª ed. São Paulo: Companhia das Letras, 2016.

LANIER, Jaron. **Dez argumentos para você deletar agora suas redes sociais**. 1ª ed. Rio de Janeiro: Intrínseca, 2018.

LIMA, Clarissa Fernandes de. **O profiling e a proteção de dados pessoais**. Monografia. Faculdade de Direito. Universidade Federal do Rio Grande Do Sul. Porto Alegre, 2019.

LOPES, Uelinton Damásio; JODARCE, Thiago. Intercepção telefônica e sua admissibilidade constitucional. **Revista Saber Digital**, v. 14, n. 2, p. 08-24, 2021.

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

\_\_\_\_\_. **A internet das coisas**. 2 ed. Rio de Janeiro: FGV Editora, 2020.

MAGRANI, Eduardo; SILVA, Priscila; VIOLA, Rafael. Novas perspectivas sobre ética e responsabilidade de inteligência artificial. In: FRAZÃO, Ana; MULHOLLAND, Caitlin de (coord.). **Inteligência artificial e direito: ética, regulação e responsabilidade**. São Paulo: Thomson Reuters Brasil, 2019, p. 115-147.

MARRAFON, Marco Aurélio; COUTINHO, Luiza Leite Cabral Loureiro. Privacy by design como princípio do direito à proteção de dados. **Conjur**. 19 jul. 2021. Disponível em: <https://www.conjur.com.br/2021-jul-19/privacy-by-design-principio-direito-protecao-dados>. Acesso em: 26 ago. 2021.

MARQUES, Claudia Lima; BAQUERO, Pablo Marcello. Primeiras impressões sobre a proposta brasileira para um marco legal da IA. **Conjur**. 24 mai. 2023. Disponível em: <https://www.conjur.com.br/2023-mai-24/garantias-consumo-impressoes-proposta-brasileira-marco-legal-ia>. Acesso em: 09 set. 2023.

MEIRELES, Adriana Veloso. Algoritmos e autonomia: relações de poder e resistência no capitalismo de vigilância. **Opinião Pública**, v. 27, n. 1, pp. 28-50, 2021. Disponível em: <https://www.redalyc.org/journal/329/32967302002/html/#B33>. Acesso em: 5 set. 2023.

MORBIDELLI, Sidney. **As relações internacionais entre os Estados e a livre concorrência no mercado mundial**. Faculdade de Direito. Pontifícia Universidade Católica de São Paulo. Tese (doutorado). São Paulo, 2009. Disponível em: <https://repositorio.pucsp.br/bitstream/handle/8489/1/Sidney%20Morbideilli.pdf>. Acesso em: 05 set. 2023.

MOURA, Maurício; CORBELLINI, Juliano. **A eleição disruptiva: Por que Bolsonaro venceu**. 1 ed. Rio de Janeiro: Record, 2019.

NASCIMENTO, Mateus L. do; RUAS, Pedro H. B.; NEVES, Otaviano; ZÁRATE, Luiz H.; NOBRE, Cristiane N.. Uma análise do fator cultural em tecnologias persuasivas: um estudo de caso da rede social *Facebook*. **Brazilian Workshop on Social Network Analysis and Mining**, Belo Horizonte, v. 7, 2018. Disponível em: <https://doi.org/10.5753/brasnam.2018.3589>. Acesso em 26 ago. 2021.

NEGRI, Sérgio Marcos Carvalho de Ávila; OLIVEIRA, Samuel Rodrigues de; COSTA, Ramon Silva. O uso de tecnologias de reconhecimento facial baseadas em inteligência artificial e o Direito à proteção de dados. **RDB**. Brasília: v. 17, n. 93, p.82-103, maio/jun. 2020.

NEGRI, Sérgio Marcos Carvalho de Ávila. Personalidade, responsabilidade e classificação dos riscos na Inteligência Artificial e na robótica. **Migalhas**. 1 jul. 2021. Disponível em: <https://www.migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/347862/personalidade-responsabilidade-e-classificacao-dos-riscos-na-ia>. Acesso em: 10 set. 2023.

\_\_\_\_\_. Robôs como pessoas: a personalidade eletrônica na Robótica e na inteligência artificial. **Pensar: Revista de Ciências Jurídicas**. Fortaleza: v. 25, n. 3, 2020. Disponível em: <https://ojs.unifor.br/rpen/article/view/10178/pdf>. Acesso em: 10 set. 2023.

O'NEIL, Cathy. **Algoritmos de destruição em massa**: como o *Big Data* aumenta a desigualdade e ameaça à democracia. 1 ed. Santo André, SP: Editora Rua do Sabão, 2020.

O'NEILL, Patrick Howell. Zuckerberg diz que “privacidade é o futuro”, mas o *Facebook* vai continuar sendo o *Facebook*. **Giz Modo**. 1 mai. 2019. Disponível em: <https://gizmodo.uol.com.br/Facebook-privacidade-futuro-f8-2019/>. Acesso em: 01 abr. 2021.

PENNYCOOK, Gordon; RAND, David. Lazy, not biased: Susceptibility to partisan fake news is better explained by lack of reasoning than by motivated reasoning. **Science Direct**, v. 188, 39-50, 2019. Disponível em: <https://www.sciencedirect.com/science/article/abs/pii/S001002771830163X?via%3DiHub>. Acesso em: 01 abr. 2021.

PENTEADO, Cláudio Luis de Camargo; SANTOS, Marcelo Burgos Pimentel dos; ARAÚJO, Rafael Aguiar de Paula; SILVA, Sidney Jard da. Ação política na internet brasileira. **Perspectivas em Ciência da Informação**, v.16, n.1, p.111-132, jan./mar. 2011.

PIMENTEL, José Eduardo de Souza. Introdução ao Direito Digital. **Revista jurídica**. São Paulo, v. 13, 2018, p. 16-39.

PINHEIRO, Patrícia Peck. **Direito Digital**. 7 ed. São Paulo: Saraiva Educação, 2021.

PINHO, José Antonio Gomes de. Investigando portais de governo Eletrônico de estados no Brasil: muita tecnologia, pouca democracia. **Revista de Administração Pública**, Rio de Janeiro, v. 42, n. 3, p. 471–493, mai. 2008.

POMPEU, Ana Luiza Brandão Calil. **Crimes Cibernéticos**: A ineficácia da Lei Carolina Dieckmann. Faculdade de Direito. Centro de educação superior de Inhumas. Monografia. Inhumas, 2022. Disponível em:

<http://65.108.49.104/bitstream/123456789/509/2/Template%20de%20TCC%20Direito%202021%20%281%29.docx.pdf>. Acesso em: 05 set. 2021.

QUEIROZ, Rafael Mafei Rabelo; FERFEBAUM, Marina. **Metodologia da Pesquisa em Direito**: técnicas e abordagens para elaboração de monografias, dissertações e teses. 2 ed. São Paulo: Saraiva, 2019.

RAIS, Diogo. SALES, Stela Rocha. Fake News, deepfake e eleições. In: RAIS, Diogo. **Fake News**: a conexão entre desinformação e o direito. 2 ed. São Paulo: Thomsom Reuters Brasil, 2020. p. 25 - 52.

RAMOS, Pedro Henrique Soares. **Neutralidade da rede**: a regulação da arquitetura da internet no Brasil. São Paulo: Editora IASP, 2018.

RENNÓ, Lúcio. Bolsonarismo e as eleições de 2022. **Estudos Avançados**, v. 36, n. 106, p. 147–163, set. 2022.

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

\_\_\_\_\_. Some Remarks on Surveillance today. **European Journal of Law and Technology**, v. 4., n. 2, 2013. Disponível em: <https://ejlt.org/index.php/ejlt/article/view/277/388>. Acesso em: 10 mai. 2021.

ROSA, Ana Cristina. Desinformação e eleições: a comunicação como instrumento estratégico. In: RAIS, Diogo. **Fake News**: a conexão entre desinformação e o direito. 2 ed. São Paulo: Thomsom Reuters Brasil, 2020. p. 53 - 64.

ROSSINI, Luiz Amélio Sodaite; SILVA, Renan Ricardo de Polli; SOTTO, Eder Carlos Salazar; ARAÚJO, Liriane Soares de. Data Mining: conceitos e consequências. **Revista Interface Tecnológica**, Taquaritinga, v. 15, n. 2, p. 50–59, 2018. DOI: 10.31510/inf.v15i2.486. Disponível em: <https://revista.fatectq.edu.br/interfacetecnologica/article/view/486>. Acesso em: 6 set. 2023.

RUSSEL, Stuart; NORVIN, Peter. **Inteligência Artificial**. Rio de Janeiro: Elsevier, 2013.

SANCHES, Pedri Nachbar; CURIATI, Eduardo Salim. A imprescindibilidade da criação da Autoridade Nacional de Proteção de Dados Pessoais (ANPD). **Migalhas**. 2 jan. 2019. Disponível em: <https://www.migalhas.com.br/depeso/293587/a-imprescindibilidade-da-criacao-da-autoridade-nacional-de-protecao-de-dados-pessoais--anpd>. Acesso em 01 set. 2023.

SENADO. Jair Bolsonaro é eleito presidente do Brasil. **Senado**. Brasília, 28 out. 2018. Disponível em: <https://www12.senado.leg.br/noticias/materias/2018/10/28/jair-bolsonaro-e-eleito-presidente-do-brasil>. Acesso em: 07 set. 2023.

\_\_\_\_\_. Lula é eleito presidente da República pela terceira vez. **Senado**. Brasília, 30 out. 2022. Disponível em: <https://www12.senado.leg.br/noticias/materias/2022/10/30/lula-e-eleito-presidente-da-republica-pela-terceira-vez>. Acesso em: 07 set. 2023.

SHANE, Tommy. The psychology of misinformation: Why we're vulnerable. **First Draft News**. 30 jun. 2020. Disponível em: <https://firstdraftnews.org/latest/the-psychology-of-misinformation-why-were-vulnerable/>. Acesso em: 29 mar. 2021.

SHUMPETER, Joseph A. **Capitalismo, socialismo e democracia**. São Paulo: Ed. Unesp, 2017.

SILVA, André Bessa da. *Big Data*, mineração de dados e aprendizagem de máquina: formas de extrair informação em grandes volumes de dados. **Revista Dimensão Acadêmica**, v. 4, n. 2, jul./dez. 2019. Disponível em: <https://multivix.edu.br/wp-content/uploads/2020/07/revista-dimensao-academica-v04-n02-artigo05.pdf>. Acesso em: 5 set. 2023.

SILVEIRA, S. A. Discursos sobre regulação e governança algorítmica. **Estudos de Sociologia**. Araraquara, v. 25, n. 48, 2020. DOI: 10.52780/res.13530. Disponível em: <https://periodicos.fclar.unesp.br/estudos/article/view/13530>. Acesso em: 11 set. 2023.

SNOWDEN, Edward. **Eterna vigilância**: como montei e desvendei o maior sistema de espionagem do mundo. São Paulo: Planeta do Brasil, 2019.

SUMPTER, David. **DOMINADOS PELOS NÚMEROS**: do *Facebook* e *Google* às fake News os algoritmos que controlam nossa vida. Rio de Janeiro: Bertrand Brasil, 2019.

TR-GO, Tribunal Regional Eleitoral de Goiás. Fato ou Boato: Justiça Eleitoral desmentiu as principais fake news sobre o processo eleitoral em 2022. **TR-GO**. Goiânia, 29 out. 2022. Disponível em: <https://www.tre-go.jus.br/comunicacao/noticias/2022/Outubro/fato-ou-boato-justica-eleitoral-desmentiu-as-principais-fake-news-sobre-o-processo-eleitoral-em-2022#:~:text=O%20relato%20falso%2C%20que%20surgiu,dos%20equipament os%20utilizados%20em%202022>. Acesso em: 05 set. 2023.

WAACK, William. Fake News: uma visão político-jornalística. In: ABOUD, Georges; NERY JR., Nelson; CAMPOS, Ricardo. **Fake News e Regulação**. 2 ed. São Paulo: Thomsom Reuters Brasil, 2020. p. 225-230.

WU, Tim. **Império da comunicação**: do telefone à internet, da AT&T ao *Google*. Rio de Janeiro: Zahar, 2012.

VISCARDI, Janaisa Martins. Fake News, verdade e mentira sob a ótica de Jair Bolsonaro no Twitter. **Trabalhos em Linguística Aplicada**. Campinas, v. 59, n. 2, p. 1134–1157, mai. 2020. Disponível em:

<https://www.scielo.br/j/tla/a/HWYM3LcW7yVtMY9ZbK8CWzs/?format=pdf&lang=pt>. Acesso em: 05 set. 2023.

ZAMPIER, Bruno. **Bens digitais**: cybercultura, redes sociais, e-mails, músicas, livros, milhas aéreas, moedas virtuais. 2 ed. Indaiatuba: Editora Foco, 2021.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira do poder. 1ª ed. Rio de Janeiro: Intrínseca, 2020.