



**CENTRO DE EDUCAÇÃO SUPERIOR CESREI - LTDA**  
**CESREI FACULDADE**  
**CURSO DE BACHARELADO EM DIREITO**

**JULIELE RODRIGUES BRANDÃO AGOSTINHO**

**ENTRE DADOS E ALGORITMOS: REFLEXOS E PARÂMETROS LEGAIS DO**  
**USO DE DADOS PESSOAIS POR MEIO DE SISTEMAS DE INTELIGÊNCIA**  
**ARTIFICIAL (IA)**

Campina Grande - PB

2023

**JULIELE RODRIGUES BRANDÃO AGOSTINHO**

**ENTRE DADOS E ALGORITMOS: REFLEXOS E PARÂMETROS LEGAIS DO  
USO DE DADOS PESSOAIS POR MEIO DE SISTEMAS DE INTELIGÊNCIA  
ARTIFICIAL (IA)**

Trabalho de Conclusão de Curso (Artigo) apresentado à Coordenação do Curso de Bacharelado em Direito da Cesrei Faculdade, como requisito parcial para a obtenção do grau de Bacharel em Direito, pela referida instituição.

Orientação: Profa. Esp. Nájila Medeiros Bezerra.

Campina Grande - PB

2023

- 
- A275e Agostinho, Juliele Rodrigues Brandão.  
Entre dados e algoritmos: reflexos e parâmetros legais do uso de dados pessoais por meio de sistemas de inteligência artificial (IA) / Juliele Rodrigues Brandão Agostinho. – Campina Grande, 2023.  
34 f.
- Artigo (Bacharelado em Direito) – Cesrei Faculdade – Centro de Educação Superior Cesrei Ltda., 2023.  
"Orientação: Profa. Esp. Nájila Medeiros Bezerra".  
Referências.
1. Direito Digital. 2. Dados Pessoais – Privacidade. 3. Inteligência Artificial. 4. Sociedade em Rede. I. Bezerra, Nájila Medeiros. II. Título.

CDU 34:004.738.5(043)

**JULIELE RODRIGUES BRANDÃO AGOSTINHO**

**ENTRE DADOS E ALGORITMOS: REFLEXOS E PARÂMETROS LEGAIS DO  
USO DE DADOS PESSOAIS POR MEIO DE SISTEMAS DE INTELIGÊNCIA  
ARTIFICIAL (IA)**

Aprovado em: \_\_\_/\_\_\_/\_\_\_\_.

**BANCA EXAMINADORA**

Prof.(a) Esp. – Nájila Medeiros Bezerra – CESREI  
Orientadora

Prof.(a) Ma. – Andréa Fernandes Silvana de Oliveira – CESREI

1º Examinador(a)

Prof.(a) Me. – Diego Araújo Coutinho – CESREI

2º Examinador(a)

## AGRADECIMENTOS

“Tudo tem seu tempo determinado e há tempo para todo propósito debaixo do céu. (...) Há tempo de plantar, e tempo de colher o que se plantou” (Eclesiastes 3:2). Assim tem sido a minha biografia, um constante processo de plantação, irrigado pelo desejo de crescer e evoluir. Se hoje colho os frutos do meu esforço, é porque fui regada com generosas gotas de incentivo, coragem, experiência e conhecimento daqueles que estiveram ao meu lado, e é a eles que expresso meus agradecimentos.

Primeiramente a Deus, o autor da vida, o alicerce da minha caminhada. Ele que sempre me fortaleceu e guiou-me em cada passo.

A minha mãe, Iris, e à minha tia, Angelina, pessoas que desde o princípio acreditaram em mim, me incentivaram e fizeram o possível para me ver chegar a essa formação. Obrigada pelo apoio e o amor incondicional demonstrado. Vocês me inspiram!

Ao meu esposo, Rodrigo, pela compreensão, paciência e pelo constante incentivo. Você foi fundamental em todos os aspectos!

Ao meu irmão, Jalyson, meu padrasto, Joseildo, meus avós, Martinha e José Rodrigues, a Guida, tia Janaína e a todos meus amigos e colegas que, de forma direta ou indireta, contribuíram para minha formação.

A minha avó, Fátima, e ao meu avô, Luiz Brandão, que, mesmo não estando mais entre nós, deixaram sua marca no meu coração e seguem sendo grandes exemplos de resiliência para minha vida.

A Prof<sup>ª</sup>. Nájila Medeiros, pelos ensinamentos e orientação desta temática, assim como a todos os professores que passaram pelo meu caminho. Obrigada por toda dedicação e conhecimento compartilhado. Comigo há um pouco de cada um de vocês!

Aos funcionários da CESREI, pela presteza e humanização no atendimento.

*“O que todos devemos fazer é nos certificar que estamos usando a inteligência artificial de uma maneira que beneficie a humanidade, e não que a deteriore.”*

*Tim Cook, CEO da Apple*

## SUMÁRIO

|                                                                                                                              |           |
|------------------------------------------------------------------------------------------------------------------------------|-----------|
| <b>1 INTRODUÇÃO</b>                                                                                                          | <b>7</b>  |
| <b>2. A REMODELAÇÃO DO CONCEITO DE PRIVACIDADE E O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS</b>                               | <b>8</b>  |
| <b>3. A SOCIEDADE EM REDE</b>                                                                                                | <b>12</b> |
| <b>4. INTELIGÊNCIA ARTIFICIAL (IA), ALGORITMOS E <i>BIG DATA</i></b>                                                         | <b>16</b> |
| <b>5. O USO DE DADOS PESSOAIS POR MEIO SISTEMAS DE INTELIGÊNCIA ARTIFICIAL (IA) E SEUS REFLEXOS NO DIREITO À PRIVACIDADE</b> | <b>21</b> |
| <b>6. A LGPD COMO PARÂMETRO JURÍDICO PARA USO DE DADOS PESSOAIS POR SISTEMA DE INTELIGÊNCIA ARTIFICIAL (IA)</b>              | <b>25</b> |
| <b>7. CONSIDERAÇÕES FINAIS</b>                                                                                               | <b>29</b> |
| <b>REFERÊNCIAS BIBLIOGRÁFICAS</b>                                                                                            | <b>30</b> |

## ENTRE DADOS E ALGORITMOS: REFLEXOS E PARÂMETROS LEGAIS DO USO DE DADOS PESSOAIS POR MEIO DE SISTEMAS DE INTELIGÊNCIA ARTIFICIAL (IA)

AGOSTINHO, Juliele Rodrigues Brandão<sup>1</sup>

BEZERRA, Nájila Medeiros<sup>2</sup>

### RESUMO

Instigada pelos efeitos que a tecnologia da inteligência artificial tem trazido à sociedade em rede, o presente estudo teve por objetivo analisar eventuais impactos que o uso de dados pessoais por meio de sistemas de inteligência artificial pode trazer à privacidade e à proteção de dados pessoais do indivíduo, buscando compreender parâmetros legais existentes que visem equilibrar o avanço tecnológico e a proteção destes bens juridicamente protegidos. Para tanto, a pesquisa caminhou sobre o viés descritivo-exploratório, sob delineamento bibliográfico e abordagem qualitativa. A temática é atual e ganha ainda mais relevância à medida que a proteção de dados pessoais e a privacidade constituem direitos fundamentais elencados na Constituição Federal de 1988, e em que as ferramentas de Inteligência Artificial e o uso de dados caracterizantes tornaram-se o principal negócios de grandes e renomadas empresas, como a Meta e o Google, mostrando-se um assunto ainda mais desafiador ao ramo do direito. Por fim, se pode inferir que a utilização de dados pessoais por sistemas inteligentes tem trazido reflexos significativos no âmbito da privacidade de seus titulares, de modo que observou-se que a Lei Geral de Proteção de Dados Pessoais emerge como um importante marco regulatório na defesa da privacidade e dos dados pessoais, capaz de equilibrar o avanço tecnológico e a proteção desses direitos individuais.

**Palavras-chave:** Dados Pessoais. Inteligência Artificial. Privacidade. Sociedade em rede.

### ABSTRACT

Instigated by the effects that artificial intelligence technology has brought to the networked society, this study aimed to analyze possible impacts that the use of personal data through artificial intelligence systems can bring to the privacy and protection of personal data of the individual, seeking to understand existing legal parameters that aim to balance technological advancement and the protection of these legally protected assets. For that, the research walked on the descriptive-exploratory bias, with bibliographic design and qualitative approach. The theme is current and gains even more relevance as the protection of personal data and privacy constitute fundamental rights listed in the Federal Constitution of 1988, and in which Artificial Intelligence tools and the use of characterizing data have become the main business

---

<sup>1</sup> Graduanda do 10º período do Curso Bacharelado em Direito do Centro de Educação Superior Cesrei. julielerbrandao@gmail.com

<sup>2</sup> Professora orientadora. Especialista em Direito Civil e Processo Civil. najilabezerra.adv@gmail.com

of large and renowned companies, such as Meta and Google, proving to be an even more challenging subject for the field of law. Finally, it can be inferred that the use of personal data by intelligent systems has brought significant reflections on the privacy of their holders, so that it was observed that the General Law for the Protection of Personal Data emerges as an important regulatory framework in the defense of privacy and personal data, capable of balancing technological advances and the protection of individual rights.

**Keywords:** Personal data. Artificial intelligence. Privacy. Network society.

## 1 INTRODUÇÃO

A introjeção de novas tecnologias na sociedade em rede, em especial a Inteligência Artificial (IA), trouxe consigo relevantes modulações sociais, estas que vão desde as relações interpessoais, a realização de simples tarefas do dia a dia, como acender uma luz ou desbloquear um celular. Implicações de sistemas inteligentes, autônomos e de autoaprendizagem, inseridos no cotidiano de diversas pessoas, mesmo que inconscientes do seu funcionamento, para muitos.

A imersão no universo digital/virtual, antes futurista, é real. Basta um clique para adentrarmos a esse âmbito “dirigido” por algoritmos e oferecer-lhes dados pessoais, seja em uma curtida na rede social, no uso de aplicativo de transporte ou em compras na internet. Cada ação na rede mundial de computadores, é capaz de gerar informações, as quais proporcionam a inteligência artificial identificar padrões comportamentais, hábitos de consumo, preferências políticas, e até mesmo prever eventuais decisões de seus usuários, e influenciá-los. Assim, presume-se que os dados pessoais são para a IA, o que o alimento representa para o corpo humano: sustento.

As regalias projetadas pela Inteligência Artificial (IA) são inúmeras, mas com elas há efeitos indesejáveis, especialmente quando estar-se-á diante de uma economia movida por dados, em que a acentuação de vigilância e a captação indevida destes, podem atingir bens juridicamente protegidos, como a proteção de dados e o direito à privacidade. Nesta contextura, a presente pesquisa tem como objetivo analisar os possíveis impactos que o uso de dados caracterizantes por sistemas de inteligência artificial pode trazer à proteção da privacidade e dos dados pessoais, buscando compreender parâmetros legais existentes que visem equilibrar o avanço tecnológico e a proteção desses direitos individuais.

A matéria ganha ainda mais relevância à medida que a proteção de dados pessoais e a privacidade constituem direitos fundamentais elencados no artigo 5º, incisos X, XI, XII e LXXIX, da Constituição Federal de 1988, e em que as ferramentas de Inteligência Artificial e

o uso de dados tornaram-se o principal negócios de grandes e renomadas empresas, como a Meta e o Google, mostrando-se um assunto ainda mais desafiador ao ramo do direito. Haja vista a necessidade do desenvolvimento tecnológico e a garantia da tutela dos bens juridicamente protegidos, como o direito à privacidade e a proteção de dados.

Diante desse cenário e dos objetivos que se pretendem atingir, esta pesquisa trilha sobre o viés descritivo-exploratório, face a imprescindibilidade de verificar e descrever as peculiaridades da Inteligência Artificial, da sociedade em rede e dos dados pessoais, bem como sua legislação específica (LGPD), e a necessidade de aprofundamento, haja vista a atualidade e relevância do tema. Neste sentido, tem-se ainda, a realização de levantamento bibliográfico a partir de doutrinas, artigos acadêmicos, notícias e publicações periódicas específicas e relevantes sobre proteção de dados, privacidade e inteligência artificial.

Por fim, esta pesquisa tem abordagem qualitativa, uma vez que os objetivos postos neste estudo, possui enfoque interpretativo, em especial acerca do que dispõe a Lei Geral de Proteção de Dados sobre o uso e tratamentos destes por Inteligência Artificial.

## **2. A REMODELAÇÃO DO CONCEITO DE PRIVACIDADE E O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS**

"Morpheus: "Você acredita em destino, Neo?" Neo: "Não". Morpheus: "Por que não?" Neo: "Porque eu não gosto da ideia de não poder controlar a minha vida" (*The Matrix*, 1999). Esse parece ser reflexo de um dos atuais conteúdos relacionados ao direito à privacidade face das constantes inovações tecnológicas na sociedade em rede e a utilização do capitalismo de vigilância: o direito de controlar a própria vida, de não ser vigiado, manipulado ou influenciado, de gerenciar suas informações, sejam elas no âmbito físico ou virtual.

A proteção do direito à privacidade é abordada de forma fragmentada na Constituição Federal de 1988, abrangendo, de acordo com a doutrina, a salvaguarda dos dados pessoais tanto no meio físico quanto no digital (MAGRINI, 2019). A Carta Magna em seu artigo 5º, incisos X, XI, XII, entabula de forma clara a proteção a intimidade, a vida privada, a honra, a imagem, ao domicílio, ao sigilo de correspondência, a comunicação, e outros direitos correlatos, como fundamentais. Espécies, que se incluem sob o gênero da privacidade.

No entanto, a privacidade posta como um direito humano ocorreu muito antes disso, na década de 1950, em resposta à ruptura totalitária. A Declaração Universal dos Direitos Humanos (DUDH) abarcou, em seu artigo 12, que ninguém será objeto de ingerências em sua vida privada ou familiar, no lar ou na correspondência e tampouco de ataques à sua honra e

reputação. Expressão reproduzida de forma semelhante no Pacto Internacional de Direitos Civis e Políticos de 1966, na Convenção Americana de Direitos Humanos e no Pacto de São José da Costa Rica de 1969 (MARINHO *et al.*, 2021).

A origem mais marcante do direito à privacidade, tradicionalmente descrito como “o direito de ser deixado só” e/ou “o direito de ser deixado em paz” (*right to be let alone*), remonta ao artigo “*The Right to Privacy*”, escrito pelos advogados Warren e Brandeis em 1890 que, analisando alguns precedentes judiciais da Suprema Corte dos Estados Unidos (EUA), especialmente sobre eventuais violações à vida privada e doméstica por aparatos tecnológicos, fotografias e jornais, enfatizaram a privacidade como um direito individual, o direito de o indivíduo estar só com seus pensamentos, emoções, sem qualquer intromissão alheia. Daí a característica da privacidade, por muito tempo, como um direito negativo, o que pressupõe a abstenção do Estado de intervir na esfera privada individual (MENDES, 2014).

Nesta intelecção, Doneda (2020), destaca que o artigo de Warren e Brandeis aponta para uma mudança na base de fundamentação da proteção da privacidade, desvinculando-a unicamente do direito de propriedade, e associando-a a inviolabilidade da personalidade<sup>3</sup> (*inviolate personality*). Isto é, a proteção em torno da pessoa humana, seja ela física, intelectual ou moral, torna-se crucial na garantia de sua privacidade.

Ao longo do século XX, a transformação do papel do Estado, juntamente com a evolução tecnológica e o aumento na circulação de informações impactaram significativamente no sentido e no alcance do direito à privacidade. O direito, que antes possuía um temperamento negativo e uma conotação quase egoísta, passou a ser reconhecido como uma garantia de controle individual sobre as próprias informações e um requisito fundamental para as democracias (MENDES, 2014). Conforme aclara Rodotà (2008, p.15), vivenciou-se, nas últimas décadas, um “processo de inexorável reinvenção da privacidade”.

Um marco diferencial dessa reconceitualização do direito à privacidade é o reconhecimento da “autodeterminação informativa”, fruto do desenvolvimento jurisprudencial do Tribunal Constitucional Alemão, quando da apreciação da Lei do Censo (*Volkszählungsurteil*), em 1983, esta que buscava coletar dados dos cidadãos no intuito de fornecer à administração pública análise populacional, demográfica e econômica, incluindo o compartilhamento de dados com órgãos públicos federais.

---

<sup>3</sup> Os direitos da personalidade “são direitos subjetivos da pessoa de defender o que lhe é próprio, ou seja, a sua integridade física (vida, alimentos, próprio corpo vivo ou morto, corpo alheio vivo ou morto, partes separadas do corpo vivo ou morto); a sua integridade intelectual (liberdade de pensamento, autoria artística e literária) e sua integridade moral (honra, recato, segredo pessoal, profissional e doméstico, imagem, identidade pessoal, familiar e social). (DINIZ, 2007, p.142)

Em decisão, parcialmente inconstitucional, a Corte argumentou a existência do direito à "autodeterminação informacional", baseado na dignidade da pessoa humana<sup>4</sup> e no livre desenvolvimento da personalidade (pertencente ao conteúdo da privacidade), pela qual cabe a cada indivíduo o direito de controlar e proteger suas próprias informações. Tornando-se assim, um marco para a teoria da proteção de dados e posteriores normas internacionais (MENDES, 2014).

De acordo com o Ministro Gilmar Mendes, em seu voto constante na ADIs 6.389, 6.390, 6.393, 6.388 e 6.387, a abordagem do Tribunal Constitucional Alemão, mostrou-se paradigmática por permitir que o direito à privacidade não ficasse restrito à dicotomia entre as esferas pública e privada, mas se desenvolvesse de forma dinâmica e constantemente sensível às referências sociais e aos distintos contextos de uso, atentando-se ao avanço tecnológico.

Neste segmento, frisa-se que o progresso tecnológico e o aumento exponencial do processamento de informações, têm gradualmente reconfigurado o cenário social e, conseqüentemente, o conteúdo da privacidade, resultando em uma estruturação cada vez mais centrada na informação e, em particular, nos dados pessoais, corolário da proteção humana.

As demandas que delineiam o perfil da privacidade, já não se limitam ao direito de estar só ou à propriedade, mas abrange outros aspectos relacionados à informação pessoal e a tecnologia. Conforme expõe Doneda (2020, p. 25), “a exposição indesejada de uma pessoa aos olhos alheios se dá hoje com maior frequência através da divulgação de seus dados pessoais do que pela intrusão em sua habitação, pela divulgação de notícias a seu respeito na imprensa, pela violação de sua correspondência - enfim, pelos meios outrora “clássicos” de violação da privacidade.” Conotação reforçada por Rodotà (2008, p. 92) ao lecionar que a privacidade engloba “o direito de manter o controle sobre as próprias informações e de determinar as modalidades de construção da própria esfera privada”.

Os desafios advindos do novo corpo social, em que a hiperconectividade e o crescimento exponencial do tratamento de dados se faz presente, fez surgir o debate quanto à necessidade de regulamentação específica a fim de resguardar a proteção de dados e as garantias fundamentais, consolidando-se com a *General Data Protection Regulation – GDPR*, promulgada pelo parlamento Europeu em abril de 2016, vigente em 25 de maio de 2018.

---

<sup>4</sup>“A dignidade da pessoa humana: concede unidade aos direitos e garantias fundamentais, sendo inerente às personalidades humanas. Esse fundamento afasta a ideia de predomínio das concepções transpessoalistas de Estado e Nação, em detrimento da liberdade individual. A dignidade é um valor espiritual e moral inerente à pessoa, que se manifesta singularmente na autodeterminação consciente e responsável da própria vida e que traz consigo a pretensão ao respeito por parte das demais pessoas, constituindo-se um mínimo invulnerável que todo estatuto jurídico deve assegurar, de modo que, somente excepcionalmente, possam ser feitas limitações ao exercício dos direitos fundamentais, mas sempre sem menosprezar a necessária estima que merecem todas as pessoas enquanto seres humanos” (MORAES, 2003, p. 41).

Evidencia-se que o advento do Regulamento Geral sobre a Proteção de Dados Europeia, catalisou a normatização internacional da proteção de dados, especialmente em razão das negociações internacionais econômicas com a União Europeia, face ao surgimento de barreiras de países sem previsão legal do tema (PINHEIRO, 2018).

Nesta acepção, sob influência europeia, em âmbito nacional as discussões sobre a proteção de dados pessoais, além de ganhar proteção infraconstitucional com a promulgação da Lei nº 13.709 de 2018, Lei Geral de Proteção de Dados - LGPD, a ser discutido em tópico específico, adquiriu relevância constitucional, solidificada com a introdução do direito fundamental à proteção de dados, inclusive nos meios digitais, no artigo 5º, inciso LXIX, por meio da Emenda Constitucional (PEC) 115, de fevereiro de 2022, oriunda da PEC 17/19.

Na sessão, o Presidente do Senado Federal, Rodrigo Pacheco, reforçou a proteção de dados como uma garantia à privacidade do cidadão ao enunciar: “O novo mandamento constitucional reforça a liberdade dos brasileiros, pois ele vem instalar-se em nossa Constituição em socorro da privacidade do cidadão. As informações pessoais pertencem, de direito, ao indivíduo e a mais ninguém.”

Todavia, é relevante destacar que muito antes, em maio de 2020, o Supremo Tribunal Federal reconheceu a proteção de dados como um direito fundamental implícito, enquadrado no art. 5º, X e XII, da CF/88, através da apreciação das Ações Diretas de Inconstitucionalidades (ADIs) 6.387, 6.388, 6.389, 6.390 e 6.393. Ações que foram ajuizadas pelo Conselho Federal da Ordem dos Advogados do Brasil (CFOAB) e por quatro partidos políticos (PSB, PSDB, PSol, PCdoB), face a medida provisória 954/2020, que determinava o compartilhamento eletrônico por parte das empresas de telecomunicação, de dados pessoais de seus clientes, como nomes, números de telefone e endereços, ao Instituto Brasileiro de Geografia e Estatística (IBGE) para a realização de pesquisas domiciliares.

Na ocasião, em sede de Medida Cautelar referendada pela Ministra Rosa Weber, relatora das ADIs retromencionadas, o Supremo Tribunal Federal reconheceu o direito fundamental à proteção de dados como um direito autônomo, derivado de uma interpretação sistemática da Constituição Federal, baseada no princípio da dignidade da pessoa humana, na proteção à intimidade e à vida privada e no instrumento *habeas data*. A tese argumentativa predominante na decisão foi a da desproporcionalidade entre os dados necessários para a pesquisa e os dados exigidos pela Medida Provisória, que abrangiam a totalidade das informações pessoais de mais de 200 milhões de brasileiros.

Nesse sentido, o STF entendeu que qualquer dado capaz de identificar uma pessoa poderia ser usado para criar perfis informacionais valiosos, merecendo, portanto, proteção

constitucional. Aludida afirmação, de um direito fundamental à proteção de dados, advém da compreensão integrada da Constituição, com base no direito à garantia da pessoa humana, na proteção à intimidade e à vida privada diante dos avanços tecnológicos e no reconhecimento da importância do *habeas data* como instrumento de tutela do direito à autodeterminação informativa (FRAZÃO; CARVALHO; MILANEZ, 2022).

Observa-se, portanto, que a evolução do tratamento atribuído ao direito à privacidade, sobretudo mediante o reconhecimento da autodeterminação informacional como proteção da personalidade humana, teve relevante papel na consolidação da proteção de dados enquanto direito fundamental autônomo. Isso porque, no escopo amplo da privacidade, compreende-se a tutela dos direitos da personalidade, que abrangem também os dados pessoais.

Deste modo, em uma sociedade em que as redes tecnológicas de comunicação e as informações pessoais são protagonistas, proteger os dados pessoais é sinônimo de proteger a própria pessoa e o seu direito à privacidade. Trata-se de garantir que o indivíduo possua o direito de decidir com quem e com qual finalidade suas informações são coletadas, assegurando-lhe o controle sobre seus próprios dados (autodeterminação informacional). Afinal, no âmbito virtual, os dados pessoais representam a pessoa física.

### **3. A SOCIEDADE EM REDE**

Se olharmos ao nosso redor, é possível perceber o quanto a realidade das pessoas tornaram-se virtuais. Desde tarefas simples do nosso dia, como a forma que somos despertados, o pagamento de um boleto, a compra de um produto, a comunicação e a maneira que buscamos informações sobre o mundo, tudo parece envolver dispositivos tecnológicos. É comum, nos depararmos, ou sermos aquelas pessoas que caminham com fones de ouvidos, escutando música ou conversando com alguém distante; que digitam apressadamente em teclados, ou até aquelas que simplesmente saem segurando seus smartphones, como se extensão de seus corpos fossem. O que se nota, é que a tecnologia faz parte do nosso social, “vê-se com óculos, fala-se com teclado, ouve-se com fones” (ROSA, 2019, p. 6.)

A sociedade em rede, é prole de relevantes avanços tecnológicos no âmbito social, em especial a gênese da internet, responsável pela hiperconectividade vivenciada, uma verdadeira teia mundial, em que o convívio virtual tem ganhado cada vez mais espaço, tornando-se na maioria das vezes um imprescindível instrumento social e econômico, seja em razão do trabalho, estudo, entretenimento, ou outro.

Neste seguimento, importa destacar que o atual modelo social, constitui uma evolução

da sociedade informacional, esta que não obstante tenha ganhado força somente nos anos de 1990 com o desenvolvimento das Tecnologias de Informação e Comunicação (TICs), possui raízes no século XX, especialmente na terceira Revolução Industrial, também conhecida como a revolução técnico-científica e informacional, em que a economia tem por fundamento o tripé da informação, tecnologia e telecomunicação (DELBIANCO, 2022).

O economista Fritz Machlup foi um dos precursores no desenvolvimento do conceito da Sociedade informacional, com a publicação de *“The Production and Distribution of Knowledge in the United States”*, identificando a informação como um recurso econômico. Nesta acepção, vê-se que a sociedade informacional, refere-se a um modelo social em que a informação é seu eixo central, a matéria prima da atividade humana, ancorada nas tecnologias de informação e comunicação (TICs), o que envolve sua aquisição, armazenamento, processamento e distribuição por meios eletrônicos, não sendo estas (tecnologias), por si só, as responsáveis pela transformação da sociedade. (SILVA; TEIXEIRA, 2019)

Com a evolução tecnológica, em especial, o crescimento exponencial das redes de comunicação, fez surgir já nos primórdios do século XXI, um novo paradigma social, a Sociedade em Rede. O sociólogo Manuel Castells foi o primeiro a utilizar essa expressão, em seu livro *“A Sociedade em Rede”* (1996), para descrever a nova forma de organização social, em que as redes<sup>5</sup> tecnológicas baseadas na microeletrônica, constitui sua espinha dorsal.

Embora seja comum o uso das terminologias *“Sociedade em Rede”* e *“Sociedade da Informação”*, para caracterizar a sociedade emergente, Castells (2005) defende que esta última não se mostra adequada, isso porque a informação sempre foi parte integrante da história da sociedade, mas o que torna singular na contemporaneidade, é a forma como elas são transmitidas e armazenadas, a partir das redes.

Para Castells (2004), a constituição da atual conjuntura social decorre de três grandes e distintas características imputadas às redes de comunicação e informação. A primeira delas, é a alta capacidade de processamento de informações, sendo aptas para lidar com grandes volumes de dados, complexidade e velocidade. A segunda refere a capacidade de combinação e recombinação de informações a partir de comunicações interativas, graças à utilização das tecnologias digitais. E a terceira particularidade consiste em sua flexibilização, uma vez que se adaptam e se integram a diferentes locais e contexto.

---

<sup>5</sup>“A rede é a estrutura formal (vide Monge e Contractor, 2004). É um sistema de nós interligados. E os nós são, em linguagem formal, os pontos onde a curva se intersecta a si própria. As redes são estruturas abertas que evoluem acrescentando ou removendo nós de acordo com as mudanças necessárias dos programas que conseguem atingir os objectivos de performance para a rede.” (CASTELLS; CARDOSO, 2005, p. 20)

Neste cenário, é a sociedade em rede, um esqueleto social em que as relações sociais, por intermédio do compartilhamento de informações, a interconexão dos indivíduos e sua interdependência, são enfatizadas. Trata-se de um tecido interligado ao binômio informação-tecnologia (em redes), um potencializador do outro, variáveis no mesmo corpo (sociedade). Pertinente ao tema, Castells (2005, p. 20) aduz:

A sociedade em rede é uma estrutura social baseada em redes operadas por tecnologias de comunicação e informação fundamentadas na microelectrónica e em redes digitais de computadores que geram, processam e distribuem informação a partir de conhecimento acumulado nos nós dessas redes.

Frente a esta conjuntura, a economia capitalista ganhou uma nova roupagem, a microeconomia da interceptação de dados pessoais, mais conhecida como o capitalismo de vigilância, em que a experiência humana no universo das redes digitais é utilizada como matéria-prima gratuita para gerar dados comportamentais. Esses dados são coletados e processados por algumas das maiores empresas mundiais, como a Google, e o Facebook (Meta), pelas quais transformaram esse processo em seu principal negócio (ZUBOFF, 2021).

O matemático londrino especializado em ciência de dados, Clive Humby, já dizia que os dados são o novo petróleo, “*Data is the new oil*”, referida frase ganha ainda mais relevância na economia digital. Neste sentido, Silveira ressalta que, diante de uma sociedade em que as redes de comunicação se fazem cada vez mais presente, empresas estão investindo em tecnologias que buscam atrair a atenção dos usuários. Isso inclui o desenvolvimento de *software* que analisam o comportamento pessoal dos indivíduos, assim como ferramentas para coletar dados e observar suas atividades na internet, como o tempo de permanência nas redes, os tipos de postagem, os anúncios e cores que mais chamam atenção, entre outros enfoques. Em suas locuções, “os dados pessoais são o elemento chave para a formação de perfis de comportamento, de consumo e até de opções culturais e políticas” (SILVEIRA, 2017. p.12).

Assim, é possível dizer que no âmbito virtual, a cada clique, uma pegada pessoal é deixada e em frações de segundo ela pode ser capturada, pois todas as vezes que utilizamos a internet, se deixa um rastro digital, ou melhor, dados são coletadas e analisadas por ferramentas tecnológicas, como a *web-beacon*, que consiste em uma técnica de rastreamento incorporadas a página de web e email, para verificar o dispositivo e o conteúdo acessado pelo usuário; o *cookies*, pequenos arquivos de textos que são armazenados no dispositivo (computador, celular, tablet, etc) do usuário; a *deep packet inspection*, técnica utilizada para monitorar e inspecionar o conteúdo específico de dados que são transmitidos nas redes e os

endereços de IP (*internet protocol*), um identificador numérico atribuído a determinado dispositivo que utiliza internet (SILVEIRA, 2017).

Nesse contexto social, enredado pela otimização de informações e a crescente adoção de tecnologias digitais, uma em especial vem ganhando destaque pela sua capacidade de realizar atividades de forma autônoma a partir da coleta, processamento e armazenamento de uma grande quantidade de dados, a denominada Inteligência Artificial (IA), expressão utilizada para se referir ao intelecto demonstrado por máquinas que se assemelham à inteligência humana e que se faz cada vez mais presente em nossa sociedade.

Inspirada no exemplo de Coutinho (2020), vejamos o dia a dia de um indivíduo inserido nessa realidade: Suzi é uma professora que ministra aula em um curso de Direito de uma renomada faculdade. Todos os dias às 06 horas da manhã, Suzi é acordada ao som de sua Assistente Virtual que como um despertador personalizado abre todas as cortinas do quarto e começa a tocar sua playlist favorita, dando início a sua rotina matinal. Ela se espreguiça e vai até o banheiro, onde a água se encontra na temperatura de sua preferência. Enquanto toma café, a mesma assistente virtual passa informações sobre a previsão do tempo, as notícias e compromissos do dia e até como está o trânsito da cidade, indicando o melhor trajeto e horário de chegada ao seu trabalho, previsto para às 07:53.

No caminho, o motorista de Suzi usa a assistente de voz do seu carro para controlar o ar-condicionado e verificar o trânsito em tempo real. Enquanto isso, Suzi pega seu *smartphone*, para marcar sua consulta médica, através do aplicativo de saúde, que lhe recomenda o dia e horário que supostamente seria mais conveniente.

Ao chegar no trabalho, às 07:53, ela tem sua identidade reconhecida pelo sistema que monitora e autoriza as entradas e saídas dos funcionários. Em uma das aulas, Suzi utiliza um quadro interativo para ensinar seus alunos sobre a utilização do princípio da preponderância nos direitos fundamentais, em outra, Suzi utiliza a tecnologia do metaverso para simular a prática de uma audiência.

São 13 horas, enquanto aguarda seu motorista, Suzi desbloqueia seu *smartphone*, com o reconhecimento facial e do seu trabalho direciona as câmaras do quintal de sua casa e observa seus cachorros brincarem. Em seguida, aproveita o acesso ao seu celular e ao dar uma olhadinha em suas redes sociais se depara com diversos anúncios do presente de aniversário que deseja comprar para sua mãe e que havia pesquisado na noite anterior.

Seu motorista chega. No trajeto de volta, ela recebe uma mensagem de texto de sua assistente virtual, lembrando-lhe que havia marcado para almoçar com sua mãe em um restaurante próximo. Ao tempo em que almoça, ela se recorda do aniversário de sua colega da

época de graduação, e na rapidez utiliza o Chat GPT para criar uma mensagem de felicitações e encaminha para sua colega através do *Whatsapp* que rapidamente informa o recebimento (“vv”) e a visualização da mensagem (os “vv” azuis).

São 17 horas, Suzi, pede para seu motorista levar sua mãe para casa e, resolve agendar um carro, por meio do aplicativo do *Uber*, para buscá-la. No percurso, aproveita o tempo para ler um livro no seu leitor de *e-book* e fazer compras em lojas virtuais. O trajeto é rápido, ela chega em casa, põe sua biometria para abrir a fechadura eletrônica, e instantaneamente o registro é armazenado em um software. Ao seu comando de voz as luzes são acesas.

Após sua rotina noturna, Suzi pega seu celular e percebe que há uma notificação para avaliar o restaurante que visitou há poucas horas. Ela se aconchega em sua cama e assiste um filme na Netflix, recomendado por um sistema de inteligência artificial que analisou seus interesses e históricos de filmes já assistidos. Suzi adormece.

O cotidiano de Suzi é aquele que, em um passado não tão distante, chamava-se de ficção, a diferença é de que agora, ele é real: estamos em um mundo onde cada um nós se torna um nó em uma rede global de dados, onde nossas experiências virtuais geram dados comportamentais, frequentemente captados, processados e armazenados por sistemas de Inteligência Artificial, capazes de realizar tarefas que, até então, eram exclusivas do homem, como "aprender" e tomar decisões. Um mundo onde vigiar comportamentos tornou-se um capital, onde empresas e organizações utilizam dados pessoais para prever e moldar comportamentos em busca de lucro e vantagem competitiva.

Não é demais lembrar que “toda ação gera uma reação”. Assim, em uma sociedade em rede, em que a economia é movida a dados, estes por sua vez constituem o coração da IA, é presumível que seu uso produza reflexos legais, principalmente, quando estar-se-á diante de bens juridicamente protegidos, como o direito à privacidade e a proteção de dados, exigindo assim, o cumprimento de parâmetros jurídicos, conforme veremos adiante. Antes, necessário se faz, termos uma percepção da Inteligência Artificial.

#### **4. INTELIGÊNCIA ARTIFICIAL (IA), ALGORITMOS E *BIG DATA***

“A vida imita a arte mais do que a arte imita a vida”, afirmou o escritor Oscar Wilde no século XIX, essa expressão nunca fez tanto sentido como agora. O ano foi 1999, o filme é *Matrix*, uma obra cinematográfica de ficção científica e ação, que retrata um mundo no qual a realidade mental percebida pelas pessoas é um simulacro de um sistema de inteligência artificial, enquanto utiliza corpos humanos em cápsulas como fonte de energia. Retornaremos.

Inserida no universo das tecnologias computacionais, a Inteligência Artificial (IA), concretiza-se como uma promissora tecnologia na contemporaneidade, presente no dia a dia de grande parte da população, seja nas recomendações que recebemos de produtos, comidas, músicas, no reconhecimento facial para desbloquear nossos *smartphones*, no corretor ortográfico, ou em outros exemplos, como verificamos no cotidiano de Suzi.

Sua gênese tem premissas após a Segunda Guerra Mundial, com o artigo "*Computing Machinery and Intelligence*" (Máquinas computacionais e inteligência), de Alan Turing, conhecido como o “pai da IA”, este que abordou o conceito de máquinas que eram inteligentes. Nesta ocasião, ele idealizou o famoso “teste de turing”.<sup>6</sup> Entretanto, foi em 1956 que o termo Inteligência Artificial foi utilizado pela primeira vez, por Jonh McCarthy em sua pesquisa na Universidade de Dartmouth. Na mesma ocasião, os acadêmicos Allen Newell, Cliff Shaw e Herbert Simon, apresentaram o *Logic Theorist* (Teórico da Lógica), com o foco “na resolução de vários teoremas matemáticos do *Principia Mathematica*”, considerado o primeiro programa de Inteligência Artificial (TAULLI, 2020).

Nos anos seguintes, especialmente em 1980, com o surgimento de redes neurais e a evolução industrial tecnológica, houve um grande progresso na IA. Seu marco notável sobreveio com o programa de *Deep Blue* capaz de derrotar Garry Kasparov, campeão mundial de xadrez, graças a capacidade de aprendizagem da máquina, conhecido como a *machine learning*, trataremos adiante. Referido feito se repetiu em 2016 com o *Software AlphaGo* vencendo o campeão mundial Lee Sedol, em um jogo de tabuleiro. Desde então a IA tem se alastrado e evoluído exponencialmente (FREITAS; FREITAS 2020).

Em que pese os primórdios da IA remontam à metade do século XX, sua definição na comunidade científica é plural, uma vez que não há consenso sobre seu real significado. Mulholland e Frajhof (BARBOSA *et al.*, 2021), por exemplo, denota que a IA sustenta na ideia de que as máquinas trabalham com a finalidade de cumprir determinados propósitos, atendidos pela percepção, aprendizado e autonomia dos agentes inteligentes, de modo que a coleta de dados soma-se ao seu conhecimento inicial permitindo-lhe atuar conforme o objetivo previsto por seus idealizadores. Freitas (2020, p. 28) aduz ser a IA “um conjunto de algoritmos relativamente autônomos, emulatório da decisão humana, programados de ordem a cumprir objetivos específicos.”

---

<sup>6</sup> “Trata-se essencialmente de um jogo com três participantes: dois humanos e um computador. O avaliador, um humano, faz perguntas abertas aos outros dois (um humano, um computador), com o objetivo de determinar qual deles é o humano. Se o avaliar não puder fazer distinção, presume-se que o computador é inteligente.” (TAULLI, 2020, p.17)

Por sua vez, Coutinho (2020, p. 23) ao citar Hartmann Peixoto (2019, p. 19), leciona que “a IA pode ser observada como uma estratégia de performance, ou como delegação de funções roboticamente praticáveis, isto é, que envolvam repetição, padrões e volumes em atividades não supervisionadas, mas sempre com fundo ético e responsável”. O Grupo Independente de Peritos de Alto Nível sobre a IA (GPAN IA), criado pela comissão europeia em junho de 2018, adotou a seguinte definição para inteligência artificial:

Os sistemas de inteligência artificial (IA) são sistemas de software (e eventualmente também de hardware) concebidos por seres humanos, que, tendo recebido um objetivo complexo, atuam na dimensão física ou digital percebendo o seu ambiente mediante a aquisição de dados, interpretando os dados estruturados ou não estruturados recolhidos, raciocinando sobre o conhecimento ou processando as informações resultantes desses dados e decidindo as melhores ações a adotar para atingir o objetivo estabelecido. Os sistemas de IA podem utilizar regras simbólicas ou aprender um modelo numérico, bem como adaptar o seu comportamento mediante uma análise do modo como o ambiente foi afetado pelas suas ações anteriores. (GPAN IA, 2019, p. 50)

Observa-se que, dentre os conceitos apresentados, há uma tentativa de aproximar a tecnologia das atividades humanas. Assim, de forma geral e em uma abordagem não técnica, a expressão Inteligência Artificial se refere a sistemas, que por meio de suas técnicas apresentam comportamentos similares aos humanos. Ou seja, "inteligências" computacionais capazes de executar tarefas que até então eram exclusivas dos seres humanos, como reconhecimento de voz e imagens.

Neste sentido, ressalta-se que as atividades realizadas pela inteligência artificial pressupõem o cumprimento de um roteiro orientado por algoritmos, ou seja, uma série de instruções definidas a partir de fórmulas matemáticas e estatísticas, incubidos de guiar o comportamento do sistema. Em outras palavras e, do ponto de vista computacional, os algoritmos são regras formais, sequenciais e bem definidas, elaboradas a partir do entendimento lógico de um problema a ser resolvido pelo programador, com o objetivo de transformá-lo em um programa que possa ser tratado e executado, em que dados de entrada (*input*) são processados e transformados em dados de saída (*output*) (MANZANO, 2019).

Imagine um corpo como uma analogia funcional para a inteligência artificial. Nesse caso, os algoritmos seriam a corrente sanguínea. Assim como as artérias transportam o sangue rico em oxigênio, os algoritmos transportam os dados de entrada (*input*), que após processado de forma semelhante a como o oxigênio é transportado para o corpo, retorna através das veias com os dados de saída (*output*). Logo, é possível dizer que tal como o corpo precisa do fluxo sanguíneo para se manter, a IA precisa dos dados para se desenvolver.

Corroborando com o tema, Colombo e Goulart (BARBOSA *et al.*, 2021, p. 276) preconiza ser os dados pessoais a fonte da atividade algorítmica “Haverá inteligência artificial quando a grande quantidade de dados torne possível a identificação de novos padrões, em face de inúmeros eventos coletados, afeiando a performance do *software*.” Com efeito, é presumível que o número de dados tem impacto significativo no desempenho da IA.

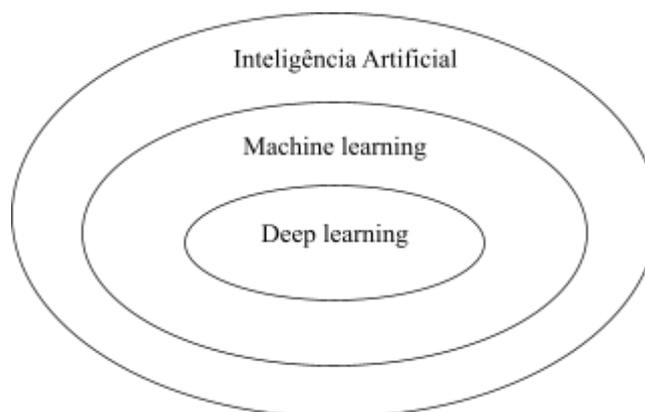
Frente ao crescente número de indivíduos conectados às redes digitais, imensuráveis dados são gerados instantaneamente. Seja através de buscas no Google, no uso de aplicativos como *WhatsApp*, nas redes sociais como Facebook e Instagram, ou até mesmo pela visualização de filmes na Netflix. Todo e qualquer movimento no universo virtual é capaz de gerar informação. Nesse contexto, o *Big Data*, como instrumento de coleta e armazenamento de grandes volumes de dados, torna-se ainda mais relevante para a Inteligência Artificial.

Como explica o professor Coutinho (2020) o *Big data* é uma categoria tecnológica que engloba o processamento de uma quantidade cada vez maior de dados, desempenhando um papel fundamental no suporte a IA, sendo, ainda, responsável pela eficácia dos algoritmos. Com o auxílio desta ferramenta, é possível operar complexos métodos de reconhecimento e análise de enormes quantidades de dados com objetivo de racionalizar decisões e eliminar intermediários (PASQUALE, 2015 *apud* CASSINO; AVELINO; SILVEIRA, 2019).

Nesta conjunção, importa destacar que os dados constituem matéria prima da informação (MENEZES; TEPEDINO, 2019). Esclareça-se, dados são ingredientes brutos, que quando processado resultam em informações, agregando maior valor nas atividades econômicas digitais. Por essa razão, a utilização de técnicas de análise massiva de dados, também conhecido como *Big Analytics*, tornaram-se tão populares entre as empresas, pois a partir destas, é possível estabelecer correlações, associações, identificar padrões e, assim, extrair informações capazes de direcionar e/ou manipular interesses de usuários.

Em essência, uma das peculiaridades da inteligência artificial, é sua capacidade de analisar dados e informações de maneira tão avançada que permite que o sistema se auto-ensine. Esse fenômeno é possível graças aos seus métodos de aprendizado como a *Machine Learning* (aprendizado da máquina) e *Deep Learning* (aprendizagem profunda), vejamos como estão estruturados, a partir da ilustração de Tom Taulli (figura 01):

**Figura 1-** Visão de alto nível dos principais componentes do mundo da IA



Fonte: Taulli, 2020, p. 35.

Observa-se que a *Machine Learning* (aprendizado da máquina) figura em uma camada tangencial da IA. Trata-se, pois, de uma técnica que permite aos algoritmos de aprendizagem executarem tarefas como reconhecimento de imagem e recomendação de produtos sem a necessidade de programação explícita a cada fim. Para tanto, mediante a captação de grande volumes de dados, o *Machine Learning* oportuniza as máquinas aprenderem automaticamente e tomarem decisões automatizadas, a exemplo de classificação automática de e-mails (spam ou não spam), análise de créditos e outros diversos.

Mulholland e Frajhof (BARBOSA *et al.*, 2021, p. 69), ao citar Selbst e Bacocas (2018, p.1094), preleciona: “A grande vantagem desta técnica é que ela é capaz de “retirar dos programadores a difícil tarefa de produzir instruções explícitas para os computadores” além de “aprender sutis entre dados que podem passar despercebidos para os humanos ou até mesmo não serem reconhecidos”.

Por sua vez, conhecida como aprendizagem profunda, a *Deep Learning* é considerada a camada submersa do *Machine Learning*. Através dessa técnica a inteligência artificial tende a aprender de forma semelhante às redes neurais humanas, proporcionando maior sofisticação a sua “inteligência”. Isso é possível através de um processamento intensivo de dados, na busca de identificar padrões que muitas vezes escapam da percepção humana (TAULLI, 2020).

Sobre essa técnica, urge trazer à lume o vocábulo de Coutinho (2020, p. 34-35):

A base de criação dessa tecnologia foi o cérebro humano, indo além das tecnologias anteriores que se limitavam a ensinar às máquinas atividades e capacidades humanas. Assim, a arquitetura cerebral foi usada como parâmetro. Foram construídas ramificações de neurônios artificiais também semelhantes aos neurônios biológicos. Dessa forma, às redes neurais não são impostas regras a serem obedecidas, mas sim dados que permitem que a própria rede identifique 35 situações padrões, onde, por meio de dados em quantidades expressivas e um poder computacional, se assemelha ao cérebro humano.

Assim, sem pretensão de esgotar o tema da inteligência artificial, propõe-se que apesar de a *Machine Learning* permitir que a IA superem algumas atividades específicas do ser humano, ainda não se tem, ao menos por enquanto, uma inteligência artificial tão autônoma, consciente e inteligente quanto a humana, uma vez que, a atual “condição tecnológica não está apta para utilizar todo o potencial que se espera da *deep learning*, pois, para que cause o impacto que se propõe, necessita de enormes quantidades de dados e de tecnologia computacional que sirva como aparato” (COUTINHO, 2020, p. 34).

Face ao exposto, vê-se que toda e qualquer atividade que envolve a inteligência artificial, os dados pessoais figuram como seu centro. Em *Matrix* (filme), a IA utiliza a energia humana como sua principal fonte de alimentação, na sociedade em rede, os dados pessoais são a fonte da inteligência artificial.

Sucedede que, contrariamente ao filme, não existem, literalmente, humanos em cápsulas sendo explorados para gerar energia, tão menos há uma batalha entre homens e máquinas na busca por sua liberdade. Os reflexos são muitos e, se apresentam de forma mais sutis como pode ser observados através do documentário "O Dilema das Redes", em que ex-funcionários e executivos de empresas como Google, Facebook e Twitter, descreve como os algoritmos de inteligência artificial coletam dados pessoais e os transformam em informações capazes de identificar, direcionar e/ou manipular os interesses dos usuários. Discutiremos.

## **5. O USO DE DADOS PESSOAIS POR MEIO SISTEMAS DE INTELIGÊNCIA ARTIFICIAL (IA) E SEUS REFLEXOS NO DIREITO À PRIVACIDADE**

Os dados pessoais são como nosso DNA, eles falam sobre nós, sobre nossas características, nossa história: seja como indivíduo ou como sociedade. Através da aplicação de inteligência artificial, com o uso de algoritmos aperfeiçoado por técnica de *Machine Learning*, é possível extrair o que Doneda (2020) chama de “metainformação”, fornecendo-o um retrato detalhado de nossos interesses, crenças, ancestralidade e outros, o que permite ao sistema conhecer futuras tendências de comportamentos e decisões de um ser, inclusive modelá-lo. Com a IA, somos um corpo virtual, formado por nossos dados pessoais.

O potencial tecnológico promovido pela sociedade em rede oferece diversas vantagens para o nosso dia a dia, como foi possível observar inicialmente no cotidiano de Suzi. No entanto, é importante reconhecer que essa mesma tecnologia é passaporte de relevantes consequências individuais e coletivas, perante a sua utilização para a vigilância e manipulação

de pessoas. À medida que a conexão e a inteligência dos bens e serviços aumentam, cresce também o patrulhamento virtual sobre nossos corpos e dados (FRAZÃO; CUEVA, 2021).

Ao que prefigura, há uma série de implicações jurídicas que podem decorrer deste cenário, especialmente no plano dos fundamentais, como a violação à privacidade e à proteção de dados pessoais, objeto deste estudo, a liberdade de expressão e outros direitos, com reflexos na dignidade da pessoa humana, princípio fundante do nosso ordenamento jurídico, em que coloca o homem como o epicentro das relações jurídicas. Referidas implicações são reforçadas, quando estar-se-á diante de uma economia impulsionada pelos dados, em que a acentuação de vigilância e o uso de técnicas de extração de informações pessoais (algoritmos de *Machine Learning*), são suas peculiaridades.

A frequente presença de algoritmos de *Machine Learning* capazes de decifrar nossas pegadas digitais, redefine o conteúdo da privacidade presente na sociedade contemporânea, atualmente, a privacidade já não se restringe à garantia de reserva do indivíduo ou seu isolamento, ela é mais, consiste na possibilidade de controlar suas informações pessoais (autodeterminação informativa) e decidir moldar a própria esfera privada (BECKER, FERRARI, 2019). Como leciona Frazão, “trata-se do poder do indivíduo de decidir sobre a divulgação e uso dos seus dados, sobre quais informações da sua vida pessoal poderiam ser divulgadas publicamente e em que condições, além de ter conhecimento sobre *quem* sabe e *o que* sabem sobre o sujeito” (FRAZÃO; CARVALHO; MILANEZ, 2022, p. 28).

Neste prisma, é possível dizer que quando um indivíduo tem seus dados violados, possivelmente sua privacidade também esteja comprometida, isso porque o direito à proteção de dados pessoais se funda na ideia de que qualquer dado é relevante, mesmo aqueles considerados públicos e que aparentemente não afetaria a esfera da vida privada podem revelar detalhes peculiares sobre os indivíduos quando agregados a outros dados (FRAZÃO; CARVALHO; MILANEZ, 2022). Para melhor elucidação destaca-se o caso da Target.

A Target, uma empresa varejista dos Estados Unidos, utilizando de sua estratégia de marketing, identificou detalhes da vida íntima de uma adolescente, antes mesmo de sua família. Por meio da coleta de dados pessoais, registros eletrônicos e o uso de técnicas de aprendizado de máquina (*Machine Learning*) e *Big Data*, a empresa traçou o perfil (*profiling*) de seus clientes, dentre eles o de gestantes, passando a fazer envios de promoções personalizadas. Neste caso específico, os anúncios da Target foram recebidos pelo pai da adolescente que, sem conhecimento da gravidez, questionou a loja o envio do material promocional para sua filha, ainda menor de idade. Contudo, tempos depois, ao entrar em contato com o pai para formalizar o pedido de desculpas, a Target tomou ciência que de fato,

a adolescente estaria grávida e a sua família só teria descoberto após confrontá-la (ALCANTARA, 2017).

Como é possível antever, a utilização do *Big data* associado aos algoritmos de *Machine Learning* possibilita ao agente de tratamento conhecimento profundo dos usuários. Para se ter uma dimensão, em uma entrevista à BBC, o especialista em *Big Data*, Martin Hilbert revelou que, com apenas 100 “curtidas” é possível prever não apenas a personalidade de um indivíduo, mas também outros aspectos, como sua orientação sexual, origem étnica, opinião religiosa e política; com 150 "curtidas", o algoritmo tem capacidade para prever sua personalidade com mais precisão do que seu parceiro; com 250 "curtidas", o algoritmo lhe conhece melhor do que você mesma. E ainda, a sua operadora de celular é capaz de rastrear sua localização por meio do seu dispositivo móvel. O Google também tem acesso a essa informação, pois você possui o Google Maps e o Gmail em seu telefone.

Todo esse conhecimento, aliado ao poder de comunicação e conexão da sociedade em rede e, alicerçado em estudos biológicos, neurocientíficos e psicológicos, pode ser intencionalmente empregado com o objetivo de manipular e/ou influenciar os usuários, inclusive, buscar modificar suas crenças (FRAZÃO, 2020). No poder do conhecimento, já não é suficiente automatizar apenas o fluxo de informações sobre nós, o objetivo agora é automatizar as nossas próprias condutas (ZUBOFF, 2019).

Neste sentido, Doneda (2020) explica que quando um perfil eletrônico é a única representação visível da personalidade de uma pessoa para outra, a sua esfera de liberdade pode ser reduzida por técnicas de previsão de comportamento. Isso porque os diversos entes com os quais se relacionam podem presumir que ela adotará um comportamento predefinido, e possivelmente limitaria suas escolhas, face a pré-determinação de algumas destas. Este fenômeno Magrini (2019) denomina-se como bolha de filtro (*filter bubble*), uma forma de customização algorítmica na navegação online que direciona produtos, serviços e anúncios específicos com base na supervisão dos nossos comportamentos em redes.

O monitoramento em questão, sem anuência, pode impactar negativamente na privacidade e por consequência na liberdade do indivíduo, uma vez que suas opiniões e visões de mundo podem ser limitadas e moldadas pelo que lhe é apresentado. A resolução (A/HRC/32/L.20) do Conselho de Direitos Humanos da ONU de 27 de junho de 2016, ao expor sobre a promoção, proteção e usufruto da internet assente: “a privacidade online é importante para a realização do direito da liberdade de expressão e para assegurar opiniões sem interferência e para o direito à liberdade de pacífica reunião ou associação.”

Como exemplo, evidencia-se o emblemático caso da *Cambridge Analytica*, no qual revelou que a empresa adquiriu de forma ilegal, sem prévio consentimento, dados pessoais de cerca 87 milhões de usuários do Facebook, incluindo suas conexões sociais, para elaborar perfis psicográficos no intuito de influenciar as escolhas dos usuários nas eleições presidenciais norte-americanas de 2016 com anúncios personalizados. Inicialmente, os dados foram coletados por meio de um teste de personalidade chamado “*This Is Your Digital Life*” que permitiu a categorização de cada indivíduo. *A posteriori*, a *Cambridge Analytica* passou a monitorar o comportamento e a navegação dos usuários dentro da plataforma, utilizando, mais uma vez, algoritmos de *Machine Learning* para determinar como cada tipo de personalidade reagia a determinadas postagens na rede social. Esse figura um dos principais debates presente no filme “A Privacidade Hackeada” (2019).

Veja-se que além de confrontar com o direito de liberdade; no caso retromencionado, a falta de transparência sobre a finalidade dos dados coletados e armazenados, bem como o monitoramento das atividades virtuais com o objetivo de traçar um perfil psicométrico dos usuários, sem devido conhecimento, configura flagrante violação, à privacidade e a proteção de dados pessoais, tutelas previstas em nossa Constituição Federal (1988), no artigo 5º, incisos X e LXXIX, respectivamente.

Sem limitar-se às plataformas digitais, insta citar o sistema da Amazon Echo, popularmente conhecido como a Alexa, que é ativado por meio de comando de voz. Ocorre que para reconhecer esses comandos, o dispositivo precisa monitorar constantemente os sons presentes no ambiente, o que significa que ele pode estar gravando vozes permanentemente. Tal recurso acarreta riscos à violação da privacidade e segurança dos usuários, tornando-os vulneráveis a possíveis ataques de hackers (MAGRINI, 2019).

Nesta conjuntura, assistimos a uma crescente tendência em que nossos dados, e, consequentemente, nossa privacidade, estão cedendo espaço em favor do entretenimento, das facilidades tecnológicas e do capitalismo de vigilância. Conforme exposto por Frazão (FRAZÃO; CARVALHO; MILANEZ, 2022) a violação à privacidade deixou de ser mero insumo das atividades econômicas, para tornar-se o próprio negócio. Quanto maior o número de dados e informações coletadas sobre indivíduos, maior é o poder econômico, político e social de seus agentes de tratamento, por sua vez, este poder tende a incentivar a contínua extração de dados, em um ciclo de retroalimentação. Em resumo, quanto menor for a importância dada ao direito à privacidade, maior será o campo de expansão da economia dos dados, ou capitalismo de vigilância.

Esse pensamento é reforçado por Zuboff (2019, p. 116):

O capitalismo de vigilância reivindica esse direito de escolha. A queixa típica é que a privacidade é erodida, mas trata-se de uma armação enganosa. No padrão social mais amplo, a privacidade não é erodida, mas redistribuída, uma vez que o direito de escolha sobre a privacidade é reivindicado pelo capital da vigilância. Em vez de as pessoas terem o direito de decidir como e o que vão revelar, esse direito é concentrado dentro do domínio do capitalismo de vigilância.

Assim, embora aparentemente sutis, a utilização excessiva de dados pessoais por sistemas de inteligência artificial implica inúmeros riscos para a privacidade, de modo que um dos principais desafios dos tempos atuais é encontrar um equilíbrio (parâmetro), entre o uso eficiente de dados pessoais, com foco em inovação e desenvolvimento econômico e tecnológico, e a proteção dos titulares desses dados. É importante que os dados sejam tratados como o novo petróleo, ou seja, com grande valor e potencial para impulsionar o avanço tecnológico, mas sem transformá-los em um novo plutônio, que pode causar danos graves individuais à sociedade como um todo (FRAZÃO; CARVALHO; MILANEZ, 2022).

## **6. A LGPD COMO PARÂMETRO JURÍDICO PARA USO DE DADOS PESSOAIS POR SISTEMA DE INTELIGÊNCIA ARTIFICIAL (IA)**

Na sociedade em rede, onde interações como reconhecimento facial, identificação por biometria, rastreamento de localização em aparelhos móveis, ativação de assistentes virtuais por voz e outros correlatos exemplos de tratamento de dados que envolvem inteligência artificial são cada vez mais frequentes, tutelar o direito à privacidade significa proteger os dados pessoais do indivíduo, permitindo-lhes exercer sua autodeterminação informativa.

Nesse contexto, embora não aborde explicitamente o uso de dados pessoais por sistemas de inteligência artificial, a Lei Geral de Proteção de Dados - LGPD, por meio de suas diretrizes, desempenha um papel fundamental como um do parâmetro jurídico na mitigação de eventuais reflexos indesejáveis no âmbito da privacidade, sendo este um dos seus principais objetivos (art.1º). Além disso, o respeito à privacidade e a autodeterminação informativa, são fundamentos legais estabelecidos pela lei (art. 2º), a serem observados em conjunto com as demais disposições, por qualquer pessoa natural ou jurídica de direito público ou privado, que processe dados pessoais em suas variadas formas, seja em meios físicos ou digitais (art.1º).

É essencial compreender que o escopo normativo da LGPD, parte do princípio de que todos os dados pessoais são relevantes, motivo pela qual adotou um conceito amplo para

dados pessoais, consistindo em qualquer “informação relacionada a pessoa natural identificada ou identificável” (art. 5º, inciso I). Para Pinheiro (2018), os dados pessoais não se restringem ao nome, sobrenome, CPF, apelido, idade, endereço residencial ou eletrônico, mas também a dados de localização, perfis de compras, número do *internet protocol* (IP), etc. Nesse sentido, destaca-se que face à peculiaridade de alguns dados capazes de revelar informações sensíveis sobre o titular, como origem racial ou étnica, convicção religiosa, opinião política, dado referente à saúde ou à vida sexual, dado genético ou biométrico e outros, a LGPD criou uma tipologia especial, nomeando-os como “dados pessoais sensíveis” em seu art. 5º, inciso II. Assim, concedeu-lhe uma proteção mais robusta.

Como visto, nas últimas décadas, o conteúdo relacionado à privacidade evoluiu para incluir o direito de o indivíduo manter o controle sobre as próprias informações, abrangendo a capacidade de a pessoa natural conhecer, controlar, direcionar e até mesmo interromper o fluxo de seus dados. Essa reconceitualização deu origem ao termo "autodeterminação informativa", desencadeada pela Corte Alemã, que representa a capacidade do indivíduo de controlar a coleta, processamento e transferência de dados (TEPEDINO; TEFFÉ, 2019).

Nesta esteira, é possível dizer que o consentimento do titular dos dados pessoais figura como ação primordial na garantia da privacidade, especialmente diante do avanço tecnológico e das conseqüentes possibilidades do uso de dados pessoais. Promover a autodeterminação informativa, como uma das formas de identificação da privacidade demonstra que, a liberdade não é sinônimo de ausência do direito, pelo contrário, conjectura como uma maneira de proteger a parte mais vulnerável da assimetria informacional<sup>7</sup>, concedendo-lhe meios efetivos que possam discernir, decidir e agir (TEPEDINO; TEFFÉ, 2019).

Neste caminho, a LGPD estabelece em seu art. 7º, inciso I e art. 11, inciso I, o consentimento do titular, como uma das formas de tratamentos de dados pessoais, as quais devem ser observadas por todas as organizações, inclusive aquelas que utilizam a IA, o que reforça sua importância como um parâmetro jurídico na proteção da privacidade. Deste modo, como um dos instrumentos profiláticos na garantia da privacidade do indivíduo, é relevante analisarmos de forma geral, o instituto do consentimento a partir de sua definição legal.

No cenário tecnológico atual, o consentimento se apresenta como uma manifestação da autonomia privada do indivíduo, revelando-se como um instrumento de expressão da escolha individual no campo dos direitos da personalidade, tendo por função autorizar o uso de dados pessoais por terceiros (DONEDA, 2020). Nesse sentido, Tepedino e Teffé (2019), revelam

---

<sup>7</sup> “Vive-se em ambiente marcado por elevada assimetria informacional: uma parte, geralmente grandes empresas e Estados, detém mais poder, recursos e melhores informações do que a outra, o cidadão comum, por vezes consumidor nas relações desenvolvidas.” (TEPEDINO; TEFFÉ, 2019, p. 90)

que atribuir natureza negocial ao consentimento seria inadequado, uma vez que reforçaria a ideia de que há uma troca entre o consentimento e uma vantagem econômica.

No regime jurídico da proteção de dados pessoais, a LGPD elucida o consentimento como uma manifestação *livre, informada e inequívoca* pela qual o titular assente com o tratamento de seus dados pessoais, estando ciente de sua *finalidade* (art. 5º, XII), devendo ser fornecido por escrito ou outro meio que demonstre a manifestação do titular (art. 8º). Noutra banda, para o tratamento de dados pessoais sensíveis, a legislação acrescenta que o consentimento deve ser fornecido de forma específica e destacada, para expressa finalidade.

*Livre*, é a liberdade dada ao titular para escolher aceitar ou recusar a utilização de seus dados, sem quaisquer pressões ou situações que possam viciar seu consentimento (art. 8º, § 3º), ou seja, permiti-lo decidir se seus dados serão tratados ou não, sem que implique em restrições de serviços e/ou bens. Nesta perspectiva, Bruno Bione (DONEDA *et al.*, 2021, p. 154), elucida que “o adjetivo livre nos remete à ideia de uma ação espontânea que não é objeto de pressão, mas, pelo contrário, de livre-arbítrio caracterizado pela tomada de uma escolha em meio a tantas outras que poderiam ser feitas por alguém.”

A título de ilustração, é possível observar em alguns portais eletrônicos uma imposição de troca, em que a navegação na plataforma é condicionada a permuta da coleta de dados pessoais, como ocorre em alguns avisos de cookies. Nesse contexto, a doutrina destaca sobre a relevância de analisar eventual assimetria de poder entre as partes, a fim de assegurar que o consentimento tenha sido provido de forma livre (TEPEDINO; TEFFÈ, 2019), isto é, verificar se no momento de sua manifestação, o titular possuía reais opções de escolhas.

A lei estabelece ainda que, se o tratamento de dados pessoais for apresentado como condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular deve ser informado com destaque sobre esse fato e os meios pelos quais seus direitos elencados no art. 18, serão exercidos (art. 9, § 3º). Acerca deste dispositivo, Tepedino e Teffé (2019) apontam ser possível interpretá-lo como uma proposta de regulação da lógica binária das denominadas políticas de tudo ou nada (*take-it-or-leave-it choice*), em que para o uso de determinado serviço, é obrigado ao usuário aceitar todas as disposições e termos ali contido.

Em tal óptica, no empenho de fortalecer a autodeterminação informativa, a LGPD possibilita a manifestação do consentimento de forma granular, permitindo que os cidadãos concedam autorizações específicas em relação ao fluxo de seus dados, ou seja, o controle dos dados pode ser fragmentado de acordo com as funcionalidades oferecidas e as necessidades de cada indivíduo, considerando os diferentes tipos de dados (TEPEDINO; TEFFÈ, 2019).

A validade do consentimento, pressupõe que o titular dos dados disponha previamente de todas as *informações* pertinentes ao seu tratamento, a fim de que possa avaliar adequadamente as circunstâncias adjacentes. “A informação é fator determinante para a expressão de um consentimento livre e consciente, circunscrito, portanto, a certo tratamento, para determinado agente e sob determinadas condições” (TEPEDINO; TEFFÈ, 2019, p. 96).

Um aspecto relevante dessa característica, ressaltado por Bioni e Luciano (2021), é a forma como as informações são transmitidas. Embora o objetivo aqui não seja analisar o cumprimento da lei por parte das empresas, mas sim demonstrar que suas diretrizes podem mitigar os impactos negativos na privacidade, é observado que, em muitos casos, os termos e políticas de privacidade se apresentam de forma extensa, com linguagem complexa, letras pequenas e designs pouco atrativos para a leitura do usuário. Essa abordagem pode levar as pessoas a consentirem sem compreender, por completo, o destino de seus dados.

Nesse sentido, é importante destacar que a legislação em apreço, ao dispor que as informações devem ser fornecidas de forma clara, adequada e ostensiva (art. 9º), correlaciona com o princípio da transparência, sendo nulo o consentimento concedido a partir de informações enganosas e/ou abusivas, vez que destoam da transparência. Assim, é direito do indivíduo estar ciente e dever do controlador fornecer informações acerca da finalidade e duração do tratamento dos dados, a identificação do responsável pelo gerenciamento do processo, a possibilidade de compartilhamentos de dados com terceiros, eventuais riscos e benefícios envolvidos no tratamento de dados, entre outras informações (art. 9º).

A validação do consentimento requer que ele seja concedido de forma *inequívoca*, clara, evidente e expressa, sem deixar margem para dúvidas quanto à escolha do indivíduo, o que afasta a possibilidade de consentimento no caso de silêncio e/ou omissão. Para Bioni e Luciano (DONEDA *et al.*, 2019) o adjetivo “*inequívoco*” está interligado ao princípio da *finalidade*, que estabelece que toda atividade de tratamento de dados deve ter um propósito específico e explícito. Assim, qualquer declaração de vontade deve ter uma direção clara, uma vez que o consentimento não pode ser dado em um vazio<sup>8</sup>.

Outra disposição relevante da LGPD que fortalece a autodeterminação informativa e, por consequência, a proteção da privacidade é a garantia de que o titular dos dados pode revogar o seu consentimento a qualquer momento, de maneira expressa e sem incorrer em

---

<sup>8</sup>“Qualquer declaração de vontade deve ter um direcionamento, já que não se concentra no vazio e de forma genérica. Seria o equivalente a emitir uma espécie de “cheque em branco” que esvaziaria qualquer esfera de controle do cidadão sobre os seus dados. Em termos práticos, o famoso “para fins de melhorar a experiência”, constante de inúmeras políticas de privacidade, deve ser abandonado”. (DONEDA *et al.*, 2019, p. 154)

quaisquer custos (art. 8º, § 5º), o que preserva a autonomia do titular em relação aos seus dados, conferindo-lhe o poder de decisão sobre a utilização de suas informações pessoais.

É importante destacar que o consentimento do titular pressupõe confiança no modo em que seus dados serão tratados. Nessa lógica, a LGPD, em seu art 46, estabelece a exigência de que os agentes responsáveis pelo tratamento de dados adotem medidas de segurança, tanto técnicas quanto administrativas, com o objetivo de proteger os dados pessoais contra acessos não autorizados, bem como contra situações acidentais ou ilícitas, desde a concepção do produto ou do serviço, até sua execução. Em outras palavras, é essencial que as empresas que tratam dados pessoais assumam a responsabilidade de proteger a privacidade e os dados dos usuários em todas as fases do desenvolvimento do produto, seja em sua arquitetura, na tecnologia empregada ou em outros aspectos relevantes.

Nota-se, portanto, que a Lei Geral de Proteção de Dados Pessoais emerge como um importante marco regulatório na defesa da privacidade e dos dados pessoais. Além de estar embasada nos princípios constitucionais, ela estabelece diretrizes claras para o uso adequado das informações pessoais, visando equilibrar o avanço tecnológico e a proteção dos direitos individuais. Deste modo, cabe às organizações e aos desenvolvedores de sistemas de inteligência artificial total observância às suas diretrizes a fim de garantir que os dados pessoais sejam tratados como um recurso valioso, isto é o novo petróleo, e não se tornem fonte de implicações negativas para seus titulares.

## **7. CONSIDERAÇÕES FINAIS**

O uso da inteligência artificial na sociedade em rede tem cada vez mais assumido uma posição de destaque, especialmente na microeconomia de interceptação de dados, também conhecido como o capitalismo de vigilância. Isso se deve ao fato de que, por meio de algoritmos aprimorados por técnicas de *Machine Learning*, é possível decifrar os rastros digitais de um indivíduo, permitindo conhecer seus interesses, analisar tendências comportamentais e eventuais decisões.

Como visto, o avanço tecnológico e o aumento exponencial do processamento de informações têm gradativamente reconfigurado o cenário social e, por consequência, redimensionado o conteúdo da privacidade. As demandas que moldam o perfil da privacidade já não se limitam ao direito de estar só, mas contemplam outros aspectos relacionados às informações, isto é, ao direito do indivíduo ter controle sobre seus dados, decidindo quais destes serão coletados, em que condições, para quem e com qual finalidade.

Dentro desse cenário, o presente estudo se propôs a analisar os potenciais impactos decorrentes do uso de dados caracterizantes por sistemas de inteligência artificial na proteção da privacidade e dos dados pessoais, buscando compreender parâmetros legais existentes que visem equilibrar o avanço tecnológico e a proteção dos direitos individuais, como a privacidade e a proteção de dados.

À luz dos fatos expostos, infere-se que a utilização de dados pessoais por sistemas inteligentes impactam de forma significativa na privacidade de seus titulares. A coleta, armazenamento e processamento de dados por meio de inteligência artificial têm potencial de retratar com detalhes interesses, crenças, preferências políticas e outras informações do indivíduo, interferindo em sua vida privada, como ocorreu no caso da Target. Além disso, a capacidade tecnológica desses sistemas é muitas vezes explorada sem conhecimento dos usuários, servindo como meio para modificar crenças, manipular e/ou influenciar pessoas, como foi exemplificado no caso da *Cambridge Analytica*. Tais práticas violam o direito fundamental à privacidade e à proteção de dados dos indivíduos.

Nesse sentido, destaca-se que a Lei Geral de Proteção de Dados Pessoais, embora não aborde especificamente o uso de dados por sistemas de inteligência artificial, representa um marco regulatório de grande importância na defesa da privacidade e dos dados pessoais, uma vez que, embasadas em princípios constitucionais elenca diretrizes capazes de promover a autodeterminação informativa e conseqüentemente a proteção da privacidade, como observou-se na previsão de tratamento de dados pessoais por meio do consentimento do titular, conferindo-lhe autonomia sobre seus próprios dados pessoais.

Portanto, é importante ter em mente que o nosso sistema legal é centrado no ser humano (antropocêntrico), o que implica que a proteção do indivíduo deve ser o átomo de todos os tipos de negócios, ou seja, diferente de *Matrix* (filme) a inteligência artificial deve estar a serviço do ser humano e nunca em prejuízo dele. Logo, a proteção da privacidade e dos dados pessoais do indivíduo devem ser colocadas no centro das atividades econômicas, e não como um diferencial destas.

## REFERÊNCIAS BIBLIOGRÁFICAS

ALCÂNTARA, Larissa Kakizaki. ***Big Data e Internet das Coisas: Desafios da Privacidade e da Proteção de Dados no Direito Digital***. São Paulo: Copyright, 2017. *E-book*.

BARBOSA, Mafalda Miranda *et al.* **Direito Digital e Inteligência Artificial: Diálogos entre Brasil e Europa.** Itaituba, São Paulo: Editora Foco, 2021.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil de 1988.** Brasília, DF: Presidência da República, [2020]. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/constituicao/constituicao.htm](http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm). Acesso em: 14 fevereiro de 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Brasília, DF: Presidência da República, [2020]. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/113709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm) Acesso em 01 de março de 2023.

BRASIL. Supremo Tribunal Federal. **Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade nº 6.387-DF.** Min. rel. Rosa Weber. Plenário, 07/05/2020, DJE 12/11/2020. Disponível em: <https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357629>. Acesso em: 21 de maio de 2023.

CASSINO, João Francisco; DA SILVA AVELINO, Rodolfo; DA SILVEIRA, Sérgio Amadeu. Direitos Humanos, inteligência artificial e privacidade. Monções: **Revista de Relações Internacionais da UFGD**, v. 8, n. 15, p. 573-596, 2019. Disponível em: [https://www.academia.edu/59625080/Direitos\\_Humanos\\_intelig%C3%A2ncia\\_artificial\\_e\\_privacidade](https://www.academia.edu/59625080/Direitos_Humanos_intelig%C3%A2ncia_artificial_e_privacidade). Acesso em: 13 de maio de 2023.

CASTELLS, Manuel; CARDOSO, Gustavo. **A Sociedade em Rede do Conhecimento à Ação Política.** Imprensa Nacional - Casa da Moeda, 2005.

CASTELLS, Manuel. **A galáxia Internet: Reflexões sobre Internet, negócios e sociedade.** Lisboa: Fundação Calouste Gulbenkian, 2004.

COUTINHO, Diego Araújo. **Direito Digital do Consumidor e Algoritmos: A Influência da Inteligência Artificial por meio de Algoritmos no poder decisório do consumidor.** Dissertação de Mestrado. Universidade Estácio de Sá. Campina Grande, 2020. Disponível em: <https://portal.estacio.br/media/4684966/diego-ara%C3%BAjo-coutinho.pdf>. Acesso em 25 de abril de 2023.

DINIZ, Maria Helena. **Curso de Direito Civil brasileiro. Teoria Geral do Direito Civil.** 24. ed. São Paulo: Saraiva, v. 1, 2007.

DELBIANCO, Natalia Rodrigues; Valentim, Marta Lígia Pomim. Sociedade da Informação e as mídias sociais contexto da comunicação científica. **AtoZ novas práticas em informação conhecimento**, v 11, p. 1-11, 2022. Disponível em: <https://revistas.ufpr.br/atoz/article/view/78778/45678>. Acesso em 18 de novembro de 2022.

DONEDA, Danilo Cesar Maganhoto. **Da Privacidade à Proteção de Dados Pessoais**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

DONEDA, Danilo *et al.* **Tratado de Dados Pessoais**. Rio de Janeiro: Forense, 2021.

GALARÇA, Sandro Lauri da Silva. **Jornalismo online na sociedade da informação. Dissertação de mestrado**. Disponível em: <https://lume.ufrgs.br/bitstream/handle/10183/5847/000432427.pdf>. Acesso em 15 de novembro de 2022

GPAN IA. **Orientações Éticas para uma IA de Confiança**. Disponível em: <https://escola.mpu.mp.br/servicos-academicos/atividades-academicas/inovaescola/curadoria/3-ciclo-de-debates/inteligencia-artificial-e-internet-das-coisas-opportunidades-e-desafios/ethicsguidelinesfortrustworthyai-ptpdf.pdf>. Acesso em 07 de maio de 2023

FRAZÃO, Ana. CARVALHO, Angelo Prata de; MILANEZ, Giovane. **Curso de Proteção de Dados - Fundamentos da LGPD**. Forense, 2022.

FRAZÃO, Ana. Plataformas digitais e o negócio de dados: necessário diálogo entre o direito da concorrência e a regulação dos dados. **Revista Direito Público**, v. 17, n. 93, p. 58-81, 2020. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3695>. Acesso em: 13 maio 2023.

\_\_\_\_\_. Plataformas Digitais, Big Data e Riscos para o Direito da Personalidade. *In*: TEPEDINO, Gustavo; MENEZES, Joyceane Bezerra de (Coord.). **Autonomia privada, liberdade existencial e direitos fundamentais**. Belo Horizonte: Fórum, 2019. 810p. ISBN 978-85-450-0585-8

FONSECA, Edson Pires. **Lei Geral de Proteção de Dados Pessoais- LGPD**. Salvador: JusPodivm, 2021.

FREITAS, Juarez; FREITAS, Thomas Bellini. **Direito e Inteligência Artificial em defesa do humano**. Belo Horizonte: Fórum, 2020.

GDPR – General Data Protection Regulation (em português) – **regulamento do Parlamento Europeu e do Conselho da União Europeia relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados**. (Regulamento Geral sobre a Proteção de Dados). 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN> Acesso em 18 de novembro de 2022.

LISSARDY, Geraldo. 'Despreparada para a era digital, a democracia está sendo destruída', afirma guru do 'big data'. **BBC**. Disponível em: <https://www.bbc.com/portuguese/geral-39535650>. Acesso em 17 de maio de 2023.

PINHEIRO, P. P. **Proteção de Dados Pessoais, comentários à Lei n. 13.709/2018 (LGPD)**. São Paulo: Saraiva, Educação, 2018.

ROSA. Munir Chahin. **A Transformação do Ser para o Direito enquanto sujeito, corpo e informação perante as Novas Tecnologias**. Trabalho de Conclusão de Curso. Faculdade de Direito, Setor de Ciências Jurídicas da Universidade Federal do Paraná. Curitiba, 2019. p. 6. Disponível em: <https://acervodigital.ufpr.br/bitstream/handle/1884/67856/TCC%20VF.pdf>. Acesso em 28 de outubro de 2022.

SILVA. Felipe Rangel; TEIXEIRA, Rodrigo Giublin. **A Sociedade da Informação e seus Desafios: A Necessidade de Efetivação de uma Política Pública de Combate ao Ransomware no Brasil**. Revista da Faculdade de Direito da UERJ - Rio de Janeiro, n. 36, Dez. 2019.

SILVEIRA, Sérgio Amadeu. **Tudo Sobre Tod@s: Redes digitais, privacidade e venda de dados pessoais**. São Paulo: Edições Sesc, 2017.

MARINHO, Gustavo *et al.* **Aspectos relevantes da Lei Geral de Proteção de Dados**. 1. ed. São Paulo: Contracorrente, 2021

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

MANZANO, José Augusto N. G. **Algoritmos: lógica para desenvolvimento de programação**. 29 ed. São Paulo: Érica, 2019.

MENDES, L. S. **Privacidade, proteção de dados e defesa do consumidor - Linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014. *E-book*.

MORAES, Alexandre de. **Direito constitucional**. 13. Ed. São Paulo: Atlas, 2003.

O DILEMA DAS REDES. Direção: Jeff Orlowski. Estados Unidos. Netflix. 2020. Disponível em: <https://www.netflix.com/br/title/81254224>. Acesso em: 16 de abril de 2023.

OIOLI, Erik. **Manual de Direito para Startups**. São Paulo (SP): Revista dos Tribunais. 2020. Disponível em: <https://thomsonreuters.jusbrasil.com.br/doutrina/1199157779/manual-de-direito-para-startups>. Acesso em: 30 de Outubro de 2022.

PRIVACIDADE HACKEADA. Direção: Karim Amer e Jehane Noujaim. Europa: Netflix, 2019. Disponível em: <https://www.netflix.com/watch/80117542?trackId=255824129>. Acesso em 25 de abril de 2023.

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

ROSA. Munir Chahin. **A Transformação do Ser para o Direito enquanto sujeito, corpo e informação perante as Novas Tecnologias**. Trabalho de Conclusão de Curso. Faculdade de Direito, Setor de Ciências Jurídicas da Universidade Federal do Paraná. Curitiba, 2019. p. 6. Disponível em: <https://acervodigital.ufpr.br/bitstream/handle/1884/67856/TCC%20VF.pdf>. Acesso em 28 de outubro de 2022.

TAULLI, Tom. **Introdução à Inteligência Artificial: Uma abordagem não técnica**. São Paulo: Novatec, 2020.

TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini. O Consentimento na Circulação de Dados Pessoais. **Revista Brasileira de Direito Civil – RBDCivil** | Belo Horizonte, v. 25, p. 83-116, jul./set. 2020. Disponível em: [https://www.academia.edu/44530563/O\\_CONSENTIMENTO\\_NA\\_CIRCULA%C3%87%C3%83O\\_DE\\_DADOS\\_PESSOAIS](https://www.academia.edu/44530563/O_CONSENTIMENTO_NA_CIRCULA%C3%87%C3%83O_DE_DADOS_PESSOAIS). Acesso em 22 de maio de 2023.

TEFFÉ, Chiara Spadaccini de. Marco Civil da Internet: considerações sobre a proteção da liberdade de expressão, neutralidade da rede e privacidade. *In*: BECKER, Daniel. FERRARI, Isabela. **Regulação 4.0: Novas tecnologias sob a perspectiva regulatória**. São Paulo: Thomson Reuters Brasil, 2019.

\_\_\_\_\_. Compliance de Dados em Tecnologia de Segurança e Vigilância. *In*: FRAZÃO, Ana. CUEVA, Ricardo Villas Bôas (Coord.). **Compliance e Políticas de Proteção de Dados**. São Paulo: Thomson Reuters Brasil, 2021.

\_\_\_\_\_. A categoria Especial dos dados sensíveis: Fundamentos e Contornos. *In*: TUFVESSON, Alessandra *et al.* **Problemas de Direito Civil**. 1. ed. Rio de Janeiro: Forense, 2021.

*The Matrix (Matrix)*, Direção e roteiro: Andy Wachowski e Larry Wachowski, produção Joel Silver, Distribuição: Warner Bros. EUA, 1999.

**United Nations General Assembly**. Human Rights Council. A/HRC/32/L.20 – Draft Resolution/Decision: The Promotion, Protection And Enjoyment Of Human Rights On The Internet., 2016. Disponível em: <https://undocs.org/Home/Mobile?FinalSymbol=A%2FHRC%2F32%2FL.20&Language=E&DeviceType=Desktop&LangRequested=False> . Acesso em 16 de maio de 2023

ZUBOFF, Shoshana. **A Era do Capitalismo de Vigilância: A Luta por um Futuro Humano na Fronteira do Poder**. Rio de Janeiro: Intrínseca, 2021. Disponível em: [https://livrogratuitosja.com/wp-content/uploads/2021/03/A-Era-do-Capitalismo-de-Vigilancia-by-Shoshana-Zuboff-z-lib.org\\_.pdf](https://livrogratuitosja.com/wp-content/uploads/2021/03/A-Era-do-Capitalismo-de-Vigilancia-by-Shoshana-Zuboff-z-lib.org_.pdf). Acesso em 14 de maio de 2023.