UNIVERSIDADE PRESBITERIANA MACKENZIE
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO POLÍTICO E ECONÔMICO

MAYARA BARTAQUINI DE SANTANNA

O IMPACTO DA INTELIGÊNCIA ARTIFICIAL NA APLICABILIDADE DA TRANSPARÊNCIA E ANONIMIZAÇÃO NA PROTEÇÃO DE DADOS

SÃO PAULO – SP
2023

MAYARA BARTAQUINI DE SANTANNA

O IMPACTO DA INTELIGÊNCIA ARTIFICIAL NA APLICABILIDADE DA TRANSPARÊNCIA E ANONIMIZAÇÃO NA PROTEÇÃO DE DADOS

Dissertação apresentada ao Programa de Pós-graduação em Direito Político e Econômico da Universidade Presbiteriana Mackenzie como requisito parcial à obtenção do título de Mestre em Direito Político e Econômico.

Orientador: Prof. Dr. Diogo Rais Rodrigues Moreira

SÃO PAULO – SP
2023

S232i Santanna, Mayara Bartaquini de.

O impacto da inteligência artificial na aplicabilidade da transparência e anonimização na proteção de dados : [recursoeletrônico]. / Mayara Bartaquini de Santanna.

Dissertação (Mestrado em Direito Político e Econômico) – Universidade Presbiteriana Mackenzie, São Paulo, 2024.

. Orientador: Prof. Dr. Diogo Rais Rodrigues Moreira.
Referências Bibliográficas: f. 116-126.

1. Inteligência artificial. Proteção de dados. 2. Aprendizado

CDDir 340.0285

Bibliotecária responsável: Jaqueline Bay Inacio Duarte- CRB-8/9509

Folha de Identificação da Agência de Financiamento

Autor: Mayara Bartaquini de Santanna

Programa de Pós-Graduação *Stricto Sensu* em Direito Político e Econômico

Título do Trabalho: O Impacto da Inteligência Artificial na Aplicabilidade da Transparência e Anonimização na Proteção de Dados

O presente trabalho foi realizado com o apoio de [1]:

☒ CAPES - Coordenação de Aperfeiçoamento de Pessoal de Nível Superior

☐ CNPq - Conselho Nacional de Desenvolvimento Científico e Tecnológico

☐ FAPESP - Fundação de Amparo à Pesquisa do Estado de São Paulo

☐ Instituto Presbiteriano Mackenzie/Isenção integral de Mensalidades e Taxas

☐ MACKPESQUISA - Fundo Mackenzie de Pesquisa

☐ Empresa/Indústria

☐ Outro:

[1] **Observação**: caso tenha usufruído mais de um apoio ou benefício, selecione-os.

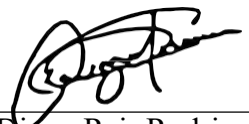
MAYARA BARTAQUINI DE SANTANNA

O IMPACTO DA INTELIGÊNCIA ARTIFICIAL NA APLICABILIDADE DATRANSPARÊNCIA E ANONIMIZAÇÃO NA PROTEÇÃO DE DADOS

Dissertação apresentada ao Programa de Pós-graduação em Direito Político e Econômico da Universidade Presbiteriana Mackenzie como requisito parcial à obtenção do título de Mestre em Direito Político e Econômico.

Aprovada em 20/02/2024

BANCA EXAMINADORA



Prof. Dr. Diogo Rais Rodrigues Moreira
Universidade Presbiteriana Mackenzie

Profa. Dra. Maria Edelvacy Pinto Marinho
Universidade Presbiteriana Mackenzie

Prof. Dr. Nikolay Henrique Bispo
Fundação Getúlio Vargas

Dedico este trabalho a Simone, Sérgio, Yvone,
Victor, Lídia, Ceciliano, Clarice e Isaura.

AGRADECIMENTOS

A Deus, pelo dom da vida, por ter segurado minhas mãos e amparado meus passos quando ninguém mais pôde. Pela luz e força concedidas para que a realização deste sonho fosse possível.

A toda minha família, pelo apoio incansável, palavras mais doces e abraços mais apertados. Por terem dividido comigo as alegrias e dores desta jornada. Com atenção especial para meus pais, Simone e Sérgio, e avós, Yvone e Victor.

Aos meus amigos, por terem me feito sorrir nos momentos em que mais precisei, por terem acreditado em mim com tanto afinco e terem sido faróis nos dias de mais escuridão. Com seleto carinho a Lilian Kadowaki, Milena Ponchio, Leonardo Leite, Ana Araújo e Patricie Barricelli.

Ao meu estimado orientador Diogo Rais, figura exemplar cuja sabedoria e dedicação são verdadeiramente inspiradoras, com quem tanto aprendi e tive a honra de conhecer ainda na graduação. Sua notável capacidade de orientação e seu comprometimento inabalável com o meu desenvolvimento acadêmico foram elementos fundamentais para o enriquecimento da minha jornada educacional.

Aos apreciados membros da banca de qualificação e defesa, Maria Marinho e Nikolay Bispo, pelos comentários engrandecedores e norteadores.

À Universidade Presbiteriana Mackenzie, minha segunda casa desde 2015, lugar em que tanto cresci como ser humano e pesquisadora.

Finalmente, expresso minha profunda gratidão à Fundação Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) pelo seu papel crucial e visionário no investimento em educação, em um país que se consolida cada vez mais como referência na busca pelo conhecimento científico. O comprometimento financeiro da CAPES não apenas representa um apoio tangível aos estudantes e pesquisadores, mas também reflete um compromisso inestimável com o progresso e a inovação.

Nós só podemos ver um pouco do futuro, mas o suficiente
para perceber que há muito a fazer.
(Alan Turing)

RESUMO

O presente trabalho aborda a evolução da inteligência artificial (IA) desde as perspectivas iniciais de Alan Turing até os avanços atuais representados pelo Chat GPT. O Capítulo 1 oferece uma visão panorâmica desses desenvolvimentos. Exploramos os fundamentos da IA, incluindo os conceitos de inteligência artificial, aprendizado de máquina e redes neurais artificiais. No Capítulo 2, concentramo-nos na proteção de dados na era da IA, a destacando como um direito fundamental. Abordamos formas de tratamento de dados, revisão de decisões automatizadas e a importância da transparência algorítmica. O Capítulo 3 explora o papel crucial da anonimização na proteção de dados no contexto da IA. Discutimos os desafios e a ameaça da reidentificação, examinando os princípios fundamentais de proteção de dados em sistemas de IA, como finalidade, minimização e prestação de contas. Também realizamos uma análise crítica dos marcos legais de proteção de dados, GDPR e LGPD, destacando desafios regulatórios na integração da IA. Ao finalizar este trabalho, reconhecemos a necessidade contínua de transparência algorítmica e interpretabilidade na regulamentação da inteligência artificial, considerando o dinamismo tecnológico. O documento visa contribuir para a compreensão e discussão sobre a interseção entre inteligência artificial e proteção de dados.

Palavras-chave: Inteligência artificial. Proteção de dados. Aprendizado de máquina. Tratamento de dados. Regulação. Princípios.

ABSTRACT

This work covers the evolution of artificial intelligence (AI) from the initial perspectives of Alan Turing to the current advances represented by Chat GPT. Chapter 1 provides an overview of these developments. We explore the foundations of AI, including the concepts of artificial intelligence, machine learning and artificial neural networks. In Chapter 2, we focus on data protection in the age of AI, highlighting it as a fundamental right. We address ways of handling data, reviewing automated decisions and the importance of algorithmic transparency. Chapter 3 explores the crucial role of anonymization in data protection in the context of AI. We discuss the challenges and threat of re-identification, examining the fundamental principles of data protection in AI systems, such as purpose, minimization and accountability. We also conducted a critical analysis of the data protection legal frameworks, GDPR and LGPD, highlighting regulatory challenges in AI integration. At the end of this work, we recognize the continued need for algorithmic transparency and interpretability in the regulation of artificial intelligence, considering technological dynamism. The paper aims to contribute to the understanding and discussion of the intersection between artificial intelligence and data protection.

Keywords: Artificial intelligence. Data protection. Machine learning. Data processing. Regulation. Principles.

LISTA DE ILUSTRAÇÕES

SUMÁRIO

INTRODUÇÃO

O advento da Inteligência Artificial (IA) marca uma era significativa na evolução tecnológica, transformando a forma como interagimos com o mundo digital e redefinindo os limites do poder cognitivo das máquinas. Este trabalho se propõe a explorar, analisar e compreender os avanços da IA, desde os primórdios, representados por Alan Turing, até as atuais capacidades, exemplificadas pelo Chat GPT. Ao longo do Capítulo 1, será traçado um panorama desses desenvolvimentos, proporcionando uma visão abrangente sobre o que impulsionou a ascensão da inteligência artificial.

Além disso, o Capítulo 1 abordará os fundamentos da IA, com ênfase nos conceitos cruciais de Aprendizado de Máquina e Redes Neurais Artificiais. Ao desmembrar o significado da inteligência artificial, aprofundaremos a compreensão sobre como máquinas podem aprender e processar informações de maneira autônoma, contribuindo para a construção de sistemas cada vez mais sofisticados.

Já no Capítulo 2, dirigiremos nosso foco para os desafios e perspectivas relacionados à proteção de dados em um cenário absorvido pela presença onipresente da IA. A proteção de dados, considerada um direito fundamental, será discutida em profundidade, destacando formas de tratamento de dados e revisão de decisões automatizadas. Adicionalmente, a transparência algorítmica, um aspecto crucial na interseção entre IA e privacidade, será explorada em detalhes.

Ao adentrar o Capítulo 3, o escopo do trabalho se estenderá para examinar a interseção entre a anonimização e a proteção de dados no contexto da IA. Questões complexas, como reidentificação e os princípios fundamentais de proteção de dados, como finalidade, minimização e prestação de contas, serão analisadas em profundidade. A investigação culminará em uma análise crítica dos marcos regulatórios, notadamente o GDPR (Regulamento Geral de Proteção de Dados) e a LGPD (Lei Geral de Proteção de Dados), que enfrentam desafios regulatórios na integração da IA.

Este trabalho visa proporcionar uma compreensão abrangente e crítica das interações entre a Inteligência Artificial e a proteção de dados, destacando os desafios enfrentados e as perspectivas emergentes neste cenário dinâmico e em constante evolução. Desta forma, consiste em um mapeamento de análise da literatura brasileira sobre os sistemas de inteligência artificial na efetividade do princípio da transparência e no procedimento de anonimização.

Por sistemas de IA entende-se modelos com poder de decisão, demais categorias apresentadas tem valor exemplificativo ou demonstrativo do alcance da tecnologia em questão.

Em relação ao princípio da transparência será abordado essencialmente o direito à explicação. Quanto ao procedimento de anonimização a exposição salienta dificuldades técnicas de sua execução plena.

Além da pesquisa bibliográfica referenciada ao longo e ao final do texto, foram consultadas as seguintes revistas: Direito Público; Revista de Direito Administrativo e Constitucional; Revista de Direito, Governança e Novas Tecnologias; *Research, Society and Development*; SBA: Controle & Automação Sociedade Brasileira de Automática; *Brazilian Archives of Biology and Technology*; Revista Ibérica de Sistemas e Tecnologias de Informação; Revista Eletrônica Científica Inovação e Tecnologia; *AI Magazine*; Revista de Direito, Estado e Telecomunicações; Revista Famecos; *Communications of the ACM*; Revista dos Tribunais; Campo Jurídico; Pensar – Revista de Ciências Jurídicas; Revista de Direito Setorial e Regulatóio; *Computer Law & Security Review*; *Behavioral and Brain Sciences*; *International Data Privacy Law*; *Proceedings on Privacy Enchancing Technologies*; *Administrative Law Review*; Revista Brasileira de Computação Aplicada; e *International Data Privacy Law.*

Assim como o banco de teses e dissertações da CAPES e a base de dados JSTOR. O marco temporal selecionado foi o posterior ao ano de 2018 (pós LGPD). Este foi respeitado sempre que possível, uma vez que, textos com o intuito de explanar o histórico da IA, por exemplo, datam de antes deste ano. Da mesma forma com publicações técnicas para aprofundar conhecimentos sobre as funcionalidades abordadas. Esta pesquisa foi atualizada até 20/03/2024.

1. A INTELIGÊNCIA ARTIFICIAL E O PODER COGNITIVO DAS MÁQUINAS

1.1 DE ALAN TURING AO CHAT GPT: UM PANORAMA SOBRE OS AVANÇOS DA INTELIGÊNCIA ARTIFICIAL

A inteligência artificial tem sido um tema em rápida expansão e despertado um interesse crescente em todo o mundo. Com avanços significativos em algoritmos, poder de processamento e grandes volumes de dados, esta tem se mostrado capaz de realizar tarefas complexas e até mesmo imitar algumas capacidades humanas.

"Podem as máquinas pensar?"[1] foi a pergunta feita por Alan Turing, em 1950, para iniciar a reflexão acerca do que viria a ser o que hoje conhecemos por inteligência artificial. Antes de adentrar o tema especificamente, o autor expõe um teste chamado de "Jogo da Imitação". Este seria jogado por três pessoas, um homem (A), uma mulher (B) e um interrogador (C), que pode pertencer a qualquer gênero.

O interrogador fica em uma sala separada dos demais e o objetivo do jogo para ele é determinar qual dos dois é o homem e qual é a mulher. Esse os conhece pelo título de "X" e "Y" e ao final do jogo pode dizer apenas "X é A e Y é B" ou o oposto "X é B e Y é A". O interrogador tem a prerrogativa de fazer perguntas para A e B e eles devem responder.

O ideal é que haja um projetor se comunicando entre as duas salas, assim as questões podem ser repetidas. O objetivo do jogo para A é fazer com que C tenha a resposta errada, entretanto, B possui como propósito ajudar C. Neste momento, Turing faz uma nova questão: o que aconteceria se um destes participantes fosse uma máquina?[2]

O autor passa a ponderar sobre que tipo de máquina está se referindo em ambas as perguntas. De modo que para ele, "[...] o interesse atual em 'máquinas pensantes' foi intensificado por um tipo particular de máquina, frequentemente chamado de 'computador eletrônico' ou 'computador digital'".[3] Para Turing, sua escolha metodológica somente seria insatisfatória se o desempenho dos computadores digitais no jogo da imitação fosse muito baixo.

Imprescindível ressaltar que o autor não estava se referindo a qualquer computador digital de seu tempo ou até mesmo assumindo que todos os computadores digitais seriam capazes de possuir um desempenho satisfatório no jogo, mas sim de um no futuro que acreditava

---

[1] TURING, Alan. Computing Machinery and Intelligence. *Mind*, volume LIX, nº 236, outubro de 1950. p. 433. Disponível em: https://www.jstor.org/stable/2251299. Acesso em: 07 abr. 2023.
[2] *Ibidem*, p. 434.
[3] *Ibidem*, p. 436.

com firmeza que existiria. Ele argumentava que as máquinas de seu tempo, embora pudessem ser consideradas universais por sua capacidade de realizar múltiplos trabalhos ao mesmo tempo, não estariam adequadas para o teste, pois não seriam capazes de imitar o pensamento humano, como uma espécie de mímica.[4]

Este argumenta que a questão de se uma máquina pode pensar está inerentemente ligada à questão de se uma máquina pode ser programada para imitar a inteligência humana de forma convincente. Sugere, portanto, que a inteligência artificial pode ser alcançada através da simulação de processos mentais humanos. Dessa forma, um sistema de computador pode ser considerado "inteligente" se for capaz de se comportar de forma indistinguível de um ser humano no Jogo da Imitação.

O pensamento, outro elemento de sua pergunta inicial, era uma grande preocupação de Turing. Para exemplificar sua visão, optou por utilizar a analogia da casca de cebola. Isto é: considerando as funções da mente e do cérebro, nos deparamos com certas operações que só podem ser explicadas por termos puramente mecânicos. Isso, para ele, não correspondia à mente real, podendo ser considerado uma camada que deve ser retirada para ser possível chegar à referida mente. Entretanto, ao retirá-la, se depararia com a uma nova camada, e assim por diante.[5]

Buscando escapar de um pensamento circular, Turing encontra uma proposta para seu problema posto. Ao invés de tentar produzir um programa para simular a mente humana adulta, por que não tentar produzir um que simularia a de uma criança?[6] Esta, afinal, sendo submetida a uma educação adequada, atingiria o cérebro adulto. O cérebro de uma criança, para fins da reflexão, poderia ser considerado uma folha em branco, facilmente programada, assumindo ainda que a quantidade de trabalho para educação de um e de outro seria a mesma.

O problema passa então a ser dividido em duas partes: o programa criança e seu processo educacional, sendo estes muito conectados. O autor tinha ciência de que não seria uma ideia simples de executar e não esperava encontrar, em suas palavras, uma boa “máquina criança” em sua primeira tentativa. Seria necessário realizar diversos testes de ensino e observar como a máquina poderia aprender.

O autor aponta que a ideia de que uma máquina pudesse aprender poderia parecer paradoxal para muitos leitores, pois poderiam questionar como as regras de operação de uma

---

[4] Imitação, para Turing, poderia ser atingida por meio de programação, desde que com uma máquina mais avançada. TURING, Alan. Computing Machinery and Intelligence. *Mind*, volume LIX, nº 236, outubro de 1950. p. 455. Disponível em: https://www.jstor.org/stable/2251299. Acesso em: 07 abr. 2023.
[5] *Ibidem*, p. 454.
[6] *Ibidem,* p. 456.

máquina poderiam mudar e sua explicação para tal é de que embora as regras de programação não mudem por si, há uma mudança muito sutil e efêmera de regras menos pretenciosas durante o processo de aprendizagem.

Pontua, por fim, que o "professor", frequentemente, durante o aprendizado da máquina, não poderá afirmar que possui conhecimento sobre o que está acontecendo internamente dessa, ainda que seja possível prever alguns de seus comportamentos.[7]

Poucos anos depois da publicação do referido artigo, no ano de 1956, na Universidade de Dartmouth, o professor da instituição John McCarthy, ao lado de Claude E. Shannon, Marvin L. Minsky, Nathaniel Rochester, foram as primeiras pessoas a utilizar o termo "inteligência artificial", no convite para uma Conferência denominada *Dartmouth Summer Research Project on Artificial Intelligence*.[8] Necessário ressaltar que neste momento os pesquisadores adotaram a concepção de Turing no que diz respeito à máquinas imitarem o comportamento humano.

No ano seguinte, Frank Rosenblatt construiu um modelo eletrônico chamado *Mark I Perceptron*. Este contava com uma rede neural analógica (o tema será abordado novamente com mais profundidade) composta por uma grade de células fotoelétricas unidas por fios a bancos de nós, contendo motores elétricos rotativos. O criador da máquina escreveu um algoritmo que a orientava a ajustar gradualmente suas forças de entrada para que pudessem identificar objetivos de maneira regular e correta, com o objetivo também de aprender.[9]

Dez anos depois da Conferência de Dartmouth, é publicado o Relatório do Comitê Consultivo para o Processamento Automático de Idiomas (ALPAC),[10] nos Estados Unidos, que apresentou conclusões pessimistas para o avanço da inteligência artificial, resultando em um grande corte de investimentos.[11] No mesmo sentido, o Relatório Lighthill, produzido no Reino Unido, argumentou acerca da dificuldade em desenvolver sistemas de inteligência artificial

---

[7] 60 anos depois da morte de Turing, a "criança robô" Eugene Goostman foi submetida ao Jogo da Imitação e obteve êxito em cerca de 30% de suas tentativas. Disponível em: https://www.zdnet.com/article/computer-chatbot-eugene-goostman-passes-the-turing-test/. Acesso em: 07 abr. 2023.

[8] MCCARTHY, J., MINSKY, M. L., ROCHESTER, N., SHANNON, C. E. A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence. *AI Magazine*, volume 27, nº 4, agosto de 1955. p. 12. Disponível em: https://doi.org/10.1609/aimag.v27i4.1904. Acesso em: 07 abr. 2023.

[9] LEFKOWITZ, Melanie. *Professor's perceptron paved the way for AI – 60 years too soon*. Cornell Chronicle, setembro de 2019. Disponível em: https://news.cornell.edu/stories/2019/09/professors-perceptron-paved-way-ai-60-years-too-soon. Acesso em: 09 abr. 2023.

[10] ALPAC. Languages and machines: computers in translation and linguistics. A report by the Automatic Language Processing Advisory Committee, Division of Behavioral Sciences, National Academy of Sciences, National Research Council. 1966, Washington: *National Academy of Sciences, National Research Council*. Disponível em: https://nap.nationalacademies.org/resource/alpac_lm/ARC000005.pdf. Acesso em: 08 abr. 2023.

[11] RICHBOURG, Robert F. *Deep Learning:* Measure Twice, Cut Once. Institute for Defense Analyses, 2018. Disponível em: http://www.jstor.org/stable/resrep36394. Acesso em: 08 abr. 2023.

capazes quanto a reconhecimento de fala e em tamanho útil ao governo.[12] Assim, o período entre o final da década de 70 e toda a de 80 foi denominado primeiro inverno da inteligência artificial em razão dos cortes de investimentos decorrentes dos relatórios mencionados.

Após o artigo de Turing, muitos outros testes foram propostos, de diferentes metodologias e com objetivos diversos também. Dentre eles, o Teste do Quarto Chinês de John Searle.[13] Relevante pontuar que o autor, diferente dos demais citados, não é um matemático, e sim um filósofo.

O teste mencionado parte das seguintes premissas: a) a intencionalidade em humanos e animais é um produto de funcionalidades causais do cérebro, assumindo isto como fato empírico sobre as relações de causa e consequência entre os processos mentais e cérebros, de maneira que simplesmente o processamento de certos cérebros é suficiente para criar intenção. b) manejar um programa de computador nunca será, por si só, uma condição suficiente para a intencionalidade; um agente humano poderia utilizar um programa e ainda assim não ter o intuito relevante; c) a explicação de como o cérebro produz uma pretensão não pode ser a mesma de manejar um programa de computador; d) qualquer mecanismo capaz de produzir intensão deve ter poderes causais iguais aos do cérebro; e) qualquer tentativa de criar intensão artificialmente não poderá obter sucesso apenas desenvolvendo programas, pois seria necessário também duplicar as forças causais do cérebro humano.

Isso posto, o teste de Searle ocorre da seguinte maneira: supondo que um falante da língua inglesa esteja em uma sala fechada repleta de símbolos chineses, esta pessoa não fala ou compreende o idioma. Existem dois buracos na parede, um por onde entram novos símbolos e um por onde devem sair de acordo com o comando da pessoa. Há ainda um livro com instruções em inglês.

Para o autor, após algumas tentativas, a pessoa seria capaz de manipular os símbolos corretamente, se apoiando em seu conhecimento adquirido com o livro de regras em sua língua nativa. Entretanto, isso não significaria que ela estaria efetivamente compreendendo o que estava fazendo, mas sim imitando o que as instruções haviam determinado, de forma a apenas substituir um símbolo por outro.

Para Searle, esta pessoa, representando uma máquina, não estaria realizando uma ação inteligente genuína, apenas reproduzindo um comportamento inteligente baseado na cópia.

---

[12] SCIENCE RESEARCH COUNCIL. *Lighthill Report:* Artificial Intelligence: a paper symposium. Reino Unido, 1973.

[13] SEARLE, John R. Minds, brains, and programs. *Behavioral And Brain Sciences*, volume 3, nº 3. P. 417-424, setembro de 1980. Cambridge University Press (CUP). Disponível em: http://dx.doi.org/10.1017/s0140525x00005756. Acesso em: 08 abr. 2023.

Assim, ainda que uma máquina passe no teste de Turing, não seria possível afirmar que o motivo foi um comportamento inteligente espontâneo ou que tenha pensado.

Um apontamento possível ao pensamento do referido autor é de que este se concentra apenas nos processos mentais baseados em linguagens e existem outras formas de inteligência que podem ser desenvolvidas por computadores. O artigo apresenta uma contribuição relevante para a associação entre inteligência artificial e a filosofia da mente, entretanto, tais entraves devem ser mencionados.

A década de 80 começou com o desenvolvimento e sucesso dos chamados "sistemas especialistas" ou "sistemas dedicados", sendo estes, máquinas que possuíam a capacidade de oferecer respostas com robusto embasamento para problemas específicos.[14] A tecnologia empolgou muitas empresas, entretanto, a necessidade de um *hardware* caro e especializado fez o movimento diminuir rapidamente, dando início ao segundo inverno da inteligência artificial.

Ao final dos anos 80, os computadores de marcas como *Apple* e *IBM* haviam dominado o mercado com as promessas de velocidade, potência e preço competitivos.[15] Cerca de 10 anos depois, em 1997, a competição de xadrez entre Gary Kasparov e o "Deep Blue", computador da *IBM*, trouxe à tona novamente o debate sobre inteligência artificial.

No ano anterior, o enxadrista havia vencido a máquina acumulando três vitórias e dois empates. A empresa, entretanto, atualizou a máquina e convidou o jogador para uma revanche em que foi derrotado com o saldo de duas derrotas e três empates.[16]

Com a chegada do século XXI e a ascensão das áreas de Ciência da Computação, Informação e Dados, houve um avanço na sofisticação da estrutura de algoritmos e *softwares*. Isso permitiu que máquinas fossem capazes de realizar tarefas que exigiam habilidades intelectuais cada vez mais complexas e com grande importância social.

No que diz respeito aos anos 2000, é possível afirmar que o tema galgou cada vez mais espaço e relevância no cenário mundial, um exemplo é a quantidade de pesquisas e publicações

---

[14] BARRETO, Luiz; PREZOTO, Marcelo. *Introdução à sistemas especialistas*. 2010. 34 f. Dissertação (Mestrado) - Curso de Mestrado em Tecnologia Para Sistemas e Fenômenos Complexos, Faculdade de Tecnologia, Universidade Estadual de Campinas, Limeira, 2010. p. 13.

[15] GONÇALVES, André Luiz Dias. *Primeiro PC da IBM foi lançado há 40 anos.* Tecmundo, agosto de 2021. Disponível em: https://www.tecmundo.com.br/produto/222975-primeiro-pc-ibm-lancado-ha-40-anos.htm e DIAS, Guilherme. *Como eram os computadores e mainframes na década de 1980.* Tecmundo, julho de 2014. Disponível em: https://www.tecmundo.com.br/supercomputadores/58611-computadores-mainframes-decada-1980-falta-imagens.htm. Acesso em: 08 abr. 2023.

[16] ALTMAN, Max. *Hoje na História:* 1996 - Kasparov derrota o computador Deep Blue da IBM. Opera Mundi, fevereiro de 2020. Disponível em: https://operamundi.uol.com.br/hoje-na-historia/9727/hoje-na-historia-1996-kasparov-derrota-o-computador-deep-blue-da-ibm. Acesso em: 08 abr. 2023.

da empresa *Google*.[17] Ao acessar o link da referência anterior e utilizar o filtro de ano, é possível perceber que em 2002 havia cinco publicações, já no ano de 2003, foram quatorze, ou seja, o número praticamente triplicou.

Em 2011, a referida empresa lançou o projeto *Google Brain* e o submeteu a um teste que condizia em avaliar dez milhões de capturas de telas do *Youtube*. A máquina foi capaz de identificar três padrões de imagens borrados: um rosto humano, um corpo humano e um gato.[18]

Mencionamos anteriormente a criação da máquina de Frank Rosenblatt que utilizava redes neurais e a importância deste acontecimento. No ano de 2012, Geoffrey Hinton, da Universidade de Toronto, em conjunto com dois alunos, criaram um modelo de rede neural profunda, chamado "Alexnet".

O objetivo era de que a rede pudesse competir em um concurso de reconhecimento de imagem, chamado "Imagenet". No concurso, os participantes foram desafiados a utilizar seus sistemas para processar milhões de imagens de teste e identificá-las com alta precisão.

A rede neural profunda, AlexNet, foi a vencedora com uma taxa de erro inferior à metade do segundo colocado. Esse resultado revelou a superioridade das redes neurais profundas em processadores gráficos em relação a outros sistemas.[19] O funcionamento da aplicação foi detalhado no artigo de seus criadores *ImageNet Classification with Deep Convolutional Neural Networks*.[20]

Outro ponto notável, a partir do final dos anos 80, é de que as empresas passaram a desenvolver pesquisas para aplicá-las a seus produtos, como a *Apple*, *IBM* e *Google*. Acima pudemos acompanhar parte da evolução do tema ao longo dos anos 2000, com ênfase nas contribuições da empresa *Google*. A ascensão do assunto é evidente na quantidade crescente de pesquisas e publicações, refletindo o interesse global nesse domínio. Em particular, o lançamento do projeto *Google Brain*, em 2011, e a conquista notável da AlexNet no concurso "Imagenet", em 2012, representam marcos significativos.

---

[17] GOOGLE RESEARCH. *Publication Database*. Disponível em: https://research.google/pubs/. Acesso em: 08 abr. 2023.

[18] FRAGA, Renê. *O que é o Google Brain e por que é tão importante na inteligência artificial?* ***Google Discovery***, fevereiro de 2023. Disponível em: https://googlediscovery.com/2023/02/20/o-que-e-o-google-brain-e-por-que-e-tao-importante-na-inteligencia-artificial/ e HISTORY OF DATA SCIENCE. *Google Brain:* The Brains Behind Your Search Engine, março de 2021. Disponível em: https://www.historyofdatascience.com/google-brain-the-brains-behind-your-search-engine/. Acesso em: 08 abr. 2023.

[19] ALAKE, Richmond. *What AlexNet Brought To The World Of Deep Learning.* Towards Data Science, julho de 2020. Disponível em: https://towardsdatascience.com/what-alexnet-brought-to-the-world-of-deep-learning-46c7974b46fc. Acesso em: 15 abr. 2023.

[20] KRIZHEVSKY, Alex; SUTSKEVER, Ilya; HINTON, Geoffrey E. Imagenet classification with deep convolutional neural networks. *Communications of the ACM*, volume 60, nº 6. P. 84-90, 2017. Disponível em: https://dl.acm.org/doi/abs/10.1145/3065386. Acesso em: 15 abr. de 2023.

O projeto *Google Brain*, ao testar a capacidade de uma máquina em identificar padrões em capturas de tela do *YouTube*, ilustra os avanços na capacidade de processamento e compreensão de dados visuais por parte da inteligência artificial. A capacidade da máquina de reconhecer padrões como rostos humanos, corpos humanos e até mesmo gatos demonstra a sofisticação alcançada na matéria.

A criação da AlexNet, uma rede neural profunda, e sua vitória no concurso "Imagenet" destacam a importância das redes neurais profundas no avanço da inteligência artificial. Essas redes se revelaram superiores em processamento de imagens, mostrando uma taxa de erro significativamente menor em comparação com outros sistemas. Esse sucesso ressalta a eficácia das abordagens baseadas em redes neurais profundas, impulsionando a pesquisa e o desenvolvimento contínuo na área de inteligência artificial.

Em 2013, um artigo foi publicado por pesquisadores da *startup* britânica *DeepMind*, mostrando como uma rede neural poderia ser utilizada para jogar e vencer 50 jogos antigos do Atari.[21] Entretanto, o DeepMind teria uma relevância ainda maior. No ano de 2016, os criadores do DeepMind levaram seu projeto para o *Google*, trocando o Atari por um jogo de tabuleiro denominado “Go”.

A partir disso estes desenvolveram um modelo de rede neural chamado “AlphaGo” para aprender e jogar o referido jogo.[22] O programa foi desafiado a jogar contra outras versões do AlphaGo, aprendendo com suas vitórias e derrotas. Isso se mostrou eficaz, e o AlphaGo acabou vencendo quatro dos cinco jogos contra o maior jogador de Go do mundo, Lee Sedol.

Pertinente mencionar que com o decurso temporal entre os testes de jogos entre máquinas e humanos, a proporção de vitórias das máquinas progrediu significativamente. A afirmação não busca comparar os testes, pois utilizaram metodologias diferentes entre si com objetivos diversos também, sendo esta uma percepção extraída da leitura das produções aqui mencionadas.

Hoje, um dos usos mais comuns da inteligência artificial é o comando de voz, presente em diversos aparelhos como computadores, celulares, TVs e principalmente nos sistemas integrados de “*smart speakers*” (uma série de microfones para os quais o usuário pode dizer seus comandos), possibilitando que uma pessoa gerencie sua casa apenas utilizando tal tecnologia.

---

[21] MNIH, Volodymyr *et al.* Playing atari with deep reinforcement learning. *ArXiv preprint arXiv:1312.5602*, 2013. Disponível em: https://arxiv.org/pdf/1312.5602v1.pdf. Acesso em: 18 abr. 2023.

[22] HASSABIS, Demis.; SULEYMAN, Mustafa.; LEGG, Shane. *DeepMind’s work in 2016:* a round-up. Google DeepMind, janeiro de 2017. Disponível em: https://www.deepmind.com/blog/deepminds-work-in-2016-a-round-up. Acesso em: 18 abr. 2023.

Este processo, no entanto, teve seu início de popularização por meio do "Iphone 4s" da marca *Apple*, lançado em 2011, e que contava com um sistema de assistente virtual. Ainda que o serviço só tenha sido habilitado no Brasil em 2014, a inovação já estava disponível desde seu lançamento nos Estados Unidos.[23]

Na década atual, a inteligência artificial foi amplamente difundida e é difícil imaginar um ponto da vida que não é tocado por ela. Desde atribuições mais simples, como sugestão de palavras no teclado do celular ou sites de busca (tal recurso funciona por estatística), que já eram utilizadas na década passada,[24] como aplicativos de música que a utilizam para recomendar conteúdo que o usuário vá interagir de maneira mais positiva.[25] Da mesma forma, em plataformas de filmes, além das sugestões personalizadas, a tecnologia também é utilizada para apresentar "capas" de filmes mais atrativas ao usuário em questão ou até mesmo cores.

Um dos temas mais debatidos envolvendo inteligência artificial nos últimos anos foi sua utilização por redes sociais para moderação de conteúdo, isto é, o acesso à informação passou a ser personalizado,[26] assim como a experiência de cada um nestas redes. Este suscitou debates em variados temas como a formação de câmaras de eco, "*fake news*", proteção de dados e, principalmente, a junção destes assuntos em um contexto eleitoral.

Fundamental destacar que a utilização mencionada acima não deve ser vista apenas por uma perspectiva negativa, pois sem este filtro a experiência do usuário poderia ser um tanto desagradável ao se deparar com uma quantidade imensa de conteúdo que não lhe interessa. Além disso, em alguns casos, não utilizar o auxílio da tecnologia seria impraticável, como o *Youtube*, por exemplo, que no ano de 2022 atingiu a marca de setecentos e oitenta e cinco milhões de usuários no mundo.[27]

Determinadas formas de utilização ainda não ocupam o imaginário coletivo de maneira alargada, como é o caso dos processos seletivos[28] ou para monitoramento de fertilidade de

---

[23] BARROS, Thiago. *O que é Siri e como usar o comando de voz do iPhone?* TechTudo, fevereiro de 2013. Disponível em: https://www.techtudo.com.br/noticias/2013/02/o-que-e-siri.ghtml. Acesso em: 08 abr. 2023.

[24] SANTINO, Renato. *Como a inteligência artificial está melhorando o teclado do seu celular.* Olhar Digital, outubro de 2015. Disponível em: https://olhardigital.com.br/2015/10/08/noticias/como-a-inteligencia-artificial-esta-melhorando-o-teclado-do-seu-celular/. Acesso em: 08 abr. 2023.

[25] OLIVEIRA, Natanael. *Spotify anuncia recurso que utiliza inteligência artificial para recomendar músicas;* entenda. CNN Brasil, fevereiro de 2023. Disponível em: https://www.cnnbrasil.com.br/economia/spotify-anuncia-recurso-que-utiliza-inteligencia-artificial-para-recomendar-musicas-entenda/. Acesso em: 08 abr. 2023.

[26] KAUFMAN, Dora; SANTAELLA, Lucia. O papel dos algoritmos de inteligência artificial nas redes sociais. *Revista Famecos*, volume 27, maio de 2020. P. 6. EDIPUCRS. Disponível em: http://dx.doi.org/10.15448/1980-3729.2020.1.34074. Acesso em: 19 abr. 2023.

[27] DEGENHARD, J. *Number of YouTube users worldwide from 2019 to 2028.* Statista, junho de 2023. Disponível em: https://www.statista.com/forecasts/1144088/youtube-users-in-the-world. Acesso em: 08 jun. 2023.

[28] BOCCIA, Sandra. *Como a inteligência artificial pode ajudar na seleção de talentos.* Época Negócios, junho de 2019. Disponível em: https://epocanegocios.globo.com/Tecnologia/noticia/2019/06/como-inteligencia-artificial-pode-ajudar-na-selecao-de-talentos.html. Acesso em: 09 abr. 2023.

animais,[29] mas essa realidade tende a ser ainda mais expandida. Uma aplicação, entretanto, que causou muitos debates é o "ChatGPT".

De acordo com seus criadores, o laboratório de pesquisas em inteligência artificial chamado "Open AI", o nome é uma sigla dos termos "*Generative Pre-Trained Transformer*". O modelo foi treinado para interagir no formato de conversas, sendo possível que o usuário formule perguntas que serão respondidas pelo "Chat". Esse também promete que a aplicação é capaz de admitir seus erros, corrigir premissas incorretas e rejeitar pedidos inapropriados.[30]

De mesma forma os criadores informam as limitações da aplicação, sendo elas: a) a possibilidade de formar respostas que soem plausíveis, mas são incorretas (sendo este um dos maiores riscos quanto a utilização da inteligência artificial, a confiança cega dos usuários de que esta não pode estar errada, ponderação que será abordada no capítulo seguinte); b) o "chat" é sensível a tentativa de inserir repetidas vezes a mesma frase ou com pequenas alterações, é sugerido que caso o usuário não consiga uma resposta na primeira tentativa busque reformular os comandos utilizados.

Continuando, c) considerando que o modelo é essencialmente verbal, este pode utilizar algumas frases repetidas; d) idealmente, o modelo deveria realizar perguntas para buscar compreender qualquer ambiguidade utilizada na solicitação do usuário, entretanto, o modelo atual apenas tenta adivinhar qual seria a opção desejada; por fim, e) apesar dos esforços de seus programadores para evitar que a aplicação responda a questões indevidas, eventualmente, tais instruções podem ser seguidas por ela, além de exibir um comportamento enviesado.

A principal diferença do "ChatGTP" para outros robôs de atendimento, denominados "chatbots", é sua capacidade de aprender. Enquanto os outros são modelos mais simples, programados para atender demandas pontuais específicas, ele possui uma capacidade de aprendizagem significativa, sendo capaz de agregar contexto para suas respostas, além de ser permitido que consulte toda a internet como fonte.

Outra aplicação muito utilizada de inteligência artificial hoje possui relação com imagens: a chamada visão computacional, isto é, a forma que sistemas interpretam e processam imagens.[31] Tal tecnologia pode ser utilizada para aumentar acessibilidade ao ser capaz de

---

[29] ÉPOCA NEGÓCIOS ONLINE. *Nestlé usa inteligência artificial para monitorar a felicidade das vacas.* Época Negócios, setembro de 2019. Disponível em: https://epocanegocios.globo.com/Tecnologia/noticia/2019/09/nestle-usa-inteligencia-artificial-para-monitorar-felicidade-das-vacas.html. Acesso em: 09 abr. 2023.
[30] OPENAI. *Introducing ChatGPT*. Disponível em: https://openai.com/blog/chatgpt. Acesso em: 08 mai. 2023.
[31] SÁ, Yuri Vasconcelos de Almeida. *Desenvolvimento de aplicações IA* – robótica, imagem e visão computacional. São Paulo: Platos Soluções Educacionais S.A., 2021, p. 6.

descrever imagens para pessoas com deficiência visual ou baixa visão, como tem sido feito pela Meta.[32]

A funcionalidade foi denominada "Texto Alternativo Automático" e funciona da seguinte forma, um leitor de tela descreve o conteúdo das imagens utilizando uma voz sintética. O leitor identifica objetos e gera descrições sob demanda, as descrições são detalhadas e personalizadas para cada imagem, com habilidade de identificar pontos de referência mundialmente famosos, atividades e tipos de animais.

Da mesma forma, o *Google Fotos* usa inteligência artificial para organizar as imagens salvas por seus usuários de maneira que, para realizar uma busca, basta apenas dizer o elemento presente na foto que deseja encontrar. Caso a busca seja por imagens com uma determinada pessoa, basta identificá-la pelo nome uma vez e realizar a pesquisa.[33]

A *Google* também possui ferramentas baseadas em visão computacional que podem ser compradas, entretanto, o foco destas é empresarial ou para desenvolvedores de aplicações.[34] Ainda, a referida tecnologia também pode ser utilizada para colaborar com outras ciências, como por exemplo as biológicas e/ou médicas, sendo possível que auxilie na medição de gordura de pacientes que não podem se levantar[35] ou que facilite demais diagnósticos.[36]

Outro ponto tocado pela inteligência artificial foram as artes e o mais recente exemplo da obra criada por uma máquina que venceu um concurso do tema.[37] Necessário ressaltar que a imagem não foi inteiramente criada com a tecnologia, um usuário gerou centenas de imagens na aplicação e escolheu as consideradas três melhores para editar em outras ferramentas. O assunto, entretanto, causou controversas entre os demais participantes e o público.

---

[32] META. *Como o Facebook está usando IA para melhorar as descrições de fotos para pessoas cegas ou com deficiência visual.* Disponível em: https://about.fb.com/br/news/2021/01/como-o-facebook-esta-usando-ia-para-melhorar-as-descricoes-de-fotos-para-pessoas-cegas-ou-com-deficiencia-visual/. Acesso em: 15 abr. 2023.

[33] BHATIA, Manjari. *Google Fotos:* inteligência para armazenar, organizar e compartilhar suas memórias. Think with Google, maio de 2017. Disponível em: https://www.thinkwithgoogle.com/intl/pt-br/estrategias-de-marketing/apps-e-mobile/google-fotos-armazenar-organizar-e-compartilhar-memorias/. Acesso em: 15 abr. 2023.

[34] API DO CLOUD VISION. Vision AI. *Google cloud*. Disponível em: https://cloud.google.com/vision?hl=pt-br#section-3. Acesso em: 15 abr. 2023.

[35] SILVA, Alexandre Gonçalves *et al*. Avaliação de gordura corporal de pacientes por visão computacional: uma revisão sistemática. *Journal of Health Informatics*, volume 12, nº 1, 2020. Disponível em: https://jhi.sbis.org.br/index.php/jhi-sbis/article/view/686. Acesso em: 08 abr. 2023.

[36] CONSTÂNCIO, A. S.; CARVALHO, D. R.; TSUNODA, D. F. Computer vision applications in healthcare: a literature review augmented with natural language processing techniques. *Research, Society and Development,* volume 11, nº 10. P. 12-13, 2022. Disponível em: https://doi.org/10.33448/rsd-v11i10.32942. Acesso em: 08 abr. 2023.

[37] GLOBO.COM. Obra feita por inteligência artificial vence concurso de arte e causa polêmica entre artistas. Globo. *Revista PEGN* – Pequenas empresas, grandes negócios. Disponível em: https://revistapegn.globo.com/Tecnologia/noticia/2022/09/obra-feita-por-inteligencia-artificial-vence-concurso-de-arte-e-causa-polemica-entre-artistas.html. Acesso em: 15 abr. 2023.

No mesmo segmento, estúdios e roteiristas estão utilizando a referida tecnologia para cooperar na escrita de roteiros de filmes e demais produções,[38] gerar novas ideias, desenvolvimento de personagens e diálogos. Essencial mencionar que essa tecnologia ainda não possui a maestria necessária para substituir humanos, sendo capaz apenas de auxiliar em tarefas consideradas burocráticas e simples. Em ambas as situações mencionadas, o humano não foi inteiramente excluído da situação, somente utilizou a tecnologia como apoio de seu processo criativo.

Este último exemplo foi alvo de grande discussão ao longo de 2023, uma vez que os roteiristas de grandes estúdios em Hollywood nos Estados Unidos entraram em greve contra o uso da inteligência artificial desta forma, dentre outras reivindicações. A greve durou cerca de 148 dias e foi finalizada com a assinatura de acordos entre os estúdios e sindicatos.

O recente pacto do WGA (sindicato da categoria) estabelece diretrizes para a utilização de inteligência artificial nas produções cinematográficas. Conforme estipulado no contrato, as empresas de produção devem comunicar aos redatores se os materiais entregues a eles foram originados por IA ou se contêm elementos gerados por essa tecnologia.

A aplicação de IA representa um aspecto delicado na indústria do entretenimento. Os estúdios desenvolveram métodos para otimizar o ciclo de desenvolvimento e produção. A rápida ascensão do ChatGPT e de outras tecnologias análogas chamou a atenção dos escritores, que percebem a "eficiência" como uma potencial ameaça ao emprego.

Conforme relatos do portal "LA Times", essa foi uma das questões finais e mais desafiadoras a serem discutidas, uma vez que tanto o sindicato quanto os estúdios relutam em comprometer-se com um acordo formulado em um cenário que pode se transformar em poucos anos.[39]

O intuito, ao apresentar esta lista razoável de exemplos, é demonstrar as capacidades e possibilidades apresentadas pela inteligência artificial e não criar situações para amedrontar o leitor. Essas são apenas algumas das principais funcionalidades da inteligência artificial, e a lista continua a crescer à medida que a tecnologia evolui e é aplicada em novas áreas e indústrias.

---

[38] DUVANEL, Talita. *Inteligência artificial é usada a sério na escrita de filmes e séries e levantam questões sobre autoria e criatividade.* O Globo, fevereiro de 2023. Disponível em: https://oglobo.globo.com/cultura/filmes/noticia/2023/02/inteligencia-artificial-e-usada-a-serio-na-escrita-de-filmes-e-series-e-levantam-questoes-sobre-autoria-e-criatividade.ghtml. Acesso em: 08 mai. 2023.

[39] OMENA, Mateus. *Greve de atores de Hollywood chega ao fim com acordo entre sindicato e estúdios.* Exame, 08 de novembro de 2023. Disponível em: https://exame.com/pop/greve-de-atores-de-hollywood-chega-ao-fim-apos-sindicato-aprovar-acordo-com-estudios/. Acesso em: 29 nov. 2023.

1.2 EXPLORANDO OS FUNDAMENTOS: O CONCEITO DE INTELIGÊNCIA ARTIFICIAL, APRENDIZADO DE MÁQUINA E REDES NEURAIS ARTIFICIAIS

1.2.1 **Conceito de inteligência artificial**

O panorama anterior pôde nos dar uma percepção abrangente sobre o caminho percorrido pela tecnologia em questão até aqui, destacando como ela está integralmente conectada aos mais diversos aspectos de nossa vida. Passaremos agora a analisar sua conceituação adotada para o referente trabalho e detalhar o funcionamento de suas principais aplicações.

John McCarthy, um dos pesquisadores a nomeá-la como inteligência artificial, propunha o seguinte conceito "[...] é a ciência ou engenharia capaz de fazer máquinas inteligentes, especialmente programas inteligentes".[40]

Certamente a definição adotada pelo pesquisador é fidedigna, a inteligência artificial é considerada uma disciplina científica que busca incorporar na máquina aspectos de inteligência, sejam eles gerais ou específicos. No entanto, considerando as proposições mencionadas por Turing e Searle, se faz necessário ponderar a respeito do que seria considerado inteligência artificial no contexto da máquina.

McCarthy, em 1987, durante o segundo inverno da inteligência artificial, criticava a falta de generalidade das máquinas específicas, para ele este era um problema latente da inteligência artificial, de modo que prejudicava desde as premissas adotas pelos estudiosos do tema até mesmo a linguagem e formação de uma base de dados.[41]

Dessa forma o autor defendia a ideia de uma linguagem para expressar o conhecimento geral da comunidade científica de modo que este pudesse ser incluído em uma base de dados geral, para que pudessem começar a deslindar um dos maiores problemas referentes a inteligência artificial para ele. Concluiu, portanto, que a autêntica inteligência artificial seria alcançada somente em uma máquina com habilidade de compreensão ampla e geral.[42]

Há uma certa tendência em associar inteligência artificial e assuntos relacionados a máquinas, de modo geral, a habilidade de seguir instruções. Entretanto, essa não poderia se

---

[40] MCCARTHY, John. *What is artificial intelligence?* Basic questions. Formal Reasoning Group, Stanford, p. 1-15, novembro de 2007. p. 2. Disponível em: http://jmc.stanford.edu/articles/whatisai.html. Acesso em: 09 abr. 2023.

[41] MCCARTHY, John. Generality in artificial intelligence. *Communications of the ACM*, volume 30, nº 12, p. 1030-1035, 1987. p. 284. Disponível em: https://dl.acm.org/doi/abs/10.1145/33447.33448. Acesso em: 09 de abr. 2023.

[42] *Ibidem*, p. 284.

configurar como a premissa mais adequada para a conceituação, pois muitas máquinas são capazes de seguir instruções sem a utilização de inteligência artificial, como por exemplo, uma calculadora. Neste exemplo, não há qualquer indício que o dispositivo em questão poderia ter relação com a tecnologia aqui discutida.

O presente trabalho não se dispõe a fazer um apanhado de conceitos e debater seus detalhes, pois seria inviável quantitativamente, mas sim encontrar uma forma de compreender a racionalidade por trás destes. Isto é, uma forma de categorizá-los para que seja possível, assim, assimilar qual aspecto está sendo privilegiado na visão apresentada.

Dessa forma, Stuart Russel e Peter Norvig contribuíram para esta distribuição do pensamento. Os autores selecionaram oito definições de inteligência artificial e as dividiram em uma tabela. A primeira linha acomoda as seguintes categorias "sistemas que pensam como humanos" (Figura 1) e "sistemas que pensam racionalmente" (Figura 2). Para eles, estas duas abarcam definições relacionadas a processos de pensamento e raciocínio.

Já a linha de baixo contém os grupos "sistemas agindo como seres humanos" (Figura 1) e "sistemas agindo racionalmente" (Figura 2), estes contemplam as noções ligadas ao comportamento. Nesse sentido, as definições da coluna esquerda, isto é, "sistemas que pensam como humanos" e "sistemas que agem como humanos" avaliam o sucesso considerando a fidelidade ao desempenho humano.

Enquanto os conceitos dispostos na coluna direita, "sistemas que pensam racionalmente" e "sistemas que agem racionalmente" mensuram o sucesso comparando-o a uma concepção de inteligência, neste caso, a racionalidade.[43] Oportuno apontar que os autores compreendem o agente racional como "[...] aquele que age para alcançar o melhor resultado ou, quando há incerteza, o melhor resultado esperado".[44]

Figura 1 – Algumas definições de inteligência artificial, organizadas em quatro categorias.

Pensando como um humano
"O novo e interessante esforço para fazer os computadores pensarem (...) *máquinas com mentes*, no sentido total e literal." (Haugeland, 1985)
"[Automatização de] atividades que associamos ao pensamento humano, atividades como a tomada de decisões, a resolução de problemas, o aprendizado..." (Bellman, 1978)
Agindo como seres humanos
"A arte de criar máquinas que executam funções que exigem inteligência quando executadas por pessoas." (Kurzweil, 1990)
"O estudo de como os computadores podem fazer tarefas que hoje são melhor desempenhadas pelas pessoas." (Rich and Knight, 1991)

Fonte: Norvig e Russel (2013).[45]

[43] NORVIG, Peter. RUSSEL, Stuart. *Inteligência Artificial***.** São Paulo: Grupo GEN, 2013. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788595156104/. Acesso em: 09 abr. 2023. p. 2.
[44] *Ibidem,* p. 5.
[45] *Ibidem*, p. 2.

Figura 2 – Algumas definições de inteligência artificial, organizadas em quatro categorias.

Pensando racionalmente
"O estudo das faculdades mentais pelo uso de modelos computacionais." (Charniak e McDermott, 1985)
"O estudo das computações que tornam possível perceber, raciocinar e agir." (Winston, 1992)
Agindo racionalmente
"Inteligência Computacional é o estudo do projeto de agentes inteligentes." (Poole *et al*., 1998)
"AI... está relacionada a um desempenho inteligente de artefatos." (Nilsson, 1998)

Fonte: Norvig e Russel (2013).[46]

A escolha destes pela abordagem racional é alvo de críticas, uma vez que nem toda escolha racional é baseada completamente em premissas corretas e por vezes a ação parte da proposição racional, mas seu resultado não acompanha esta classificação, sendo necessário uma ação posterior. Entretanto, os autores estão satisfeitos com sua escolha metodológica, pois a consideram a mais abrangente e melhor atingível na pesquisa científica.[47]

Quanto ao agir humano, os autores consideram o teste de Turing satisfatório. De modo que se o humano participante do teste na função (C) – interrogador, não for capaz de distinguir se as respostas de (A) ou (B) estão sendo geradas por uma máquina, esta estaria se comportando suficientemente como humano.[48] Assim, resta apenas um ponto a ser abordado o "pensar como um humano".

Não temos aqui uma pretensão de compreender a formação do pensamento no cérebro humano, uma vez que tal análise ultrapassa o escopo do trabalho, entretanto, podemos realizar ponderações sobre a mente e sua relação com o cérebro. A ciência responsável por aprofundar tal relação é a neurociência.[49]

Russel e Norvig fazem uma digressão em seu livro sobre o tema e apontam que embora existam dados sobre o mapeamento de áreas do cérebro e partes do corpo controladas por elas, estes podem mudar no decurso de semanas.[50] Ainda, postulam os autores "[...] não compreendemos inteiramente como outras áreas do cérebro podem assumir o comando de certas funções quando uma área é danificada".[51]

---

[46] *Ibidem.*
[47] *Ibidem*.
[48] *Ibidem*, p. 3.
[49] HERCULANO-HOUZEL, Suzana. Uma Breve História da Relação entre o Cérebro e a Mente. In: LENT, Roberto. *Neurociência:* da mente ao comportamento. São Paulo: Grupo Gen, 2008. Cap. 1, p. 2. Disponível em: https://app.minhabiblioteca.com.br/#/books/978-85-277-1994-0/. Acesso em: 09 abr. 2023.
[50] NORVIG, Peter. RUSSEL, Stuart. *Inteligência Artificial.* São Paulo: Grupo GEN, 2013. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788595156104/. Acesso em: 09 abr. 2023. p. 10.
[51] *Ibidem*.

Concluem, portanto, que "[...] uma coleção de células simples pode levar ao pensamento, à ação ou à consciência". Sendo assim, cérebros e computadores digitais têm atributos distintos e comparar o desempenho de um algoritmo na solução de uma questão ao comportamento humano é um procedimento que deve ser deixado de lado.

Existem, hoje, no Congresso Nacional, quarenta e seis Projetos de Lei debatendo regulamentação da inteligência artificial (trinta e quatro na Câmara dos Deputados e doze no Senado)[52]. Muitos deles são semelhantes e tratam de temas complementares, entretanto, o que concentra as atenções é o PL nº 2338/2023[53], que define a tecnologia como:

> Sistema computacional, com graus diferentes de autonomia, desenhado para inferir como atingir um dado conjunto de objetivos, utilizando abordagens baseadas em aprendizagem de máquina e/ou lógica e representação do conhecimento, por meio de dados de entrada provenientes de máquinas ou humanos, com o objetivo de produzir previsões, recomendações ou decisões que possam influenciar o ambiente virtual ou real.

O conceito acima, evidentemente, ainda pode ser alterado durante a tramitação do texto legal, porém foi mencionado para ilustrar sua similaridade com a definição aqui adotada. Além de evidenciar a abrangência significável, uma vez que oferece uma definição ampla e atualizada de sistema de inteligência artificial.

Ele reconhece a natureza complexa e multifacetada dos sistemas, destacando sua capacidade de inferir maneiras de atingir objetivos específicos, seja por meio de aprendizado de máquina, lógica ou representação do conhecimento. Ademais, ressalta a importância dos dados de entrada, provenientes tanto de máquinas quanto de seres humanos, na geração de previsões, recomendações ou decisões que podem impactar o ambiente virtual ou real.

Em novembro de 2023, a OCDE alterou sua definição de IA. A recente definição espelha o progresso desta tecnologia nos últimos cinco anos e será alicerce para quaisquer legislações adicionais sobre o assunto formuladas nos trinta e oito países membros da organização. A distinção principal em relação à definição prévia é que os propósitos de um sistema de IA não são obrigados a serem determinados por seres humanos, mas podem surgir internamente nas máquinas. Desta forma:

> Um sistema de IA é um sistema baseado em máquina que, para objetivos explícitos ou implícitos, infere, a partir da entrada que recebe, como gerar resultados, como previsões, conteúdo, recomendações ou decisões que podem influenciar ambientes

---

[52] AMOROZO, Marcos. Congresso tem pelo menos 46 projetos de lei para regulamentar do uso de inteligência artificial. CNN, 18 de fevereiro de 2024. Disponível em: https://www.cnnbrasil.com.br/politica/congresso-tem-pelo-menos-46-projetos-de-lei-para-regulamentar-do-uso-de-inteligencia-artificial/#:~:text=O%20PL%20regulamenta%20conceitos%2C%20fundamentos,identificados%20por%20meio%20de%20avalia%C3%A7%C3%A3o. Acesso em: 12 mar. 2024.

[53] BRASIL. Senado Federal. *Projeto de Lei nº 2338 de 2023*. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/157233#tramitacao_10494842. Acesso em: 3 mar. 2024.

> físicos ou virtuais. Diferentes sistemas de IA variam em seus níveis de autonomia e adaptabilidade após a implantação. (Traduzido pela autora).[54]

O conceito abordado acima será adotado para este trabalho, pois oferece uma visão precisa sobre o que constitui um sistema de inteligência artificial. Ele destaca a capacidade dos sistemas de IA de inferir e gerar resultados a partir de entradas específicas, podendo produzir previsões, conteúdo, recomendações ou decisões que têm o potencial de influenciar tanto ambientes físicos quanto virtuais.

Além disso, reconhece a variação nos níveis de autonomia e adaptabilidade entre diferentes sistemas refletindo a diversidade e complexidade dessas tecnologias. Essa definição é fundamental para entender o papel crescente da tecnologia abordada em diversos aspectos da sociedade contemporânea, além de servir como base para a formulação de políticas e regulamentações que garantam seu uso ético e responsável. Dessa forma o próximo tópico inicia o debate sobre as principais funcionalidades da inteligência artificial.

1.2.2 **Aprendizado de máquina e redes neurais artificiais**

Na primeira parte do presente capítulo foram apresentados diversos argumentos acerca da possibilidade de máquinas aprenderem. Neste momento, aprofundaremos tal debate demonstrando como funcionam os sistemas que propiciam os feitos demonstrados.

A metodologia de aprendizagem automática ("*machine learning*"), presente na maioria das aplicações atuais de inteligência artificial, incluindo as redes neurais profundas ("*deep learning*"), envolve a identificação de padrões em grandes conjuntos de informações, responsável pelo êxito dessas técnicas, mas também por sua vulnerabilidade.[55] A fragilidade em questão possui relação com a qualidade dos dados inseridos nos modelos, tema que será abordado no capítulo seguinte.

O procedimento de aprendizado de máquina é aquele que possibilita ao computador criar seus próprios algoritmos (por algoritmo podemos compreender a sequência de instruções

---

[54] OECD. *Recommendation of the Council on Artificial Intelligence*. Disponível em: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449. Acesso em: 10 mar. 2024.
"On the proposal of the Committee on Digital Economy Policy:
"AGREES that for the purpose of this Recommendation the following terms should be understood as follows:
–AI system: An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment."

[55] KAUFMAN, Dora. *Desmistificando a inteligência artificial*. São Paulo: Grupo Autêntica, 2022. Disponível em: https://app.minhabiblioteca.com.br/#/books/9786559281596/. Acesso em: 10 abril 2023. p. 17.

que informa ao computador o que ele deve fazer). Obviamente é necessário ter uma fonte inicial, isto é, uma pessoa que escreva o algoritmo e permita a auto-programação e adaptação. Essa fonte inicial é conhecida como algoritmo de aprendizagem.[56]

Nesse sentido, Pedro Domingos[57] possui uma explicação de fácil compreensão para tal procedimento:

> Todo algoritmo tem uma entrada e uma saída: os dados entram no computador, o algoritmo faz o que precisa com eles e um resultado é produzido. O "machine learning" faz o contrário: entram os dados e o resultado desejado e é produzido o algoritmo que transforma um no outro. Os algoritmos de aprendizado - também conhecidos como aprendizes – são aqueles que criam outros algoritmos.

Antes da introdução da Aprendizagem de Máquina, os algoritmos de inteligência artificial contavam com a habilidade da equipe de programadores em incorporar na codificação um volume suficiente de diretrizes. Uma estratégia para enfrentar esses desafios era incumbir a equipe de programação de incluir um conjunto de informações acompanhadas das respostas esperadas para cada dado, assegurando, desse modo, que o sistema computacional conseguisse derivar as diretrizes que associam os dados com as respostas. Dessa maneira, as normas estabelecidas pelo algoritmo poderiam ser aplicadas a conjuntos de dados, efetuando as previsões.[58]

Ao invés de iniciar um modelo mediante a organização de dados e estabelecimento de diretrizes previamente fixadas por um usuário humano, a Aprendizagem de Máquina encara o processo de descoberta de conhecimento e formulação de regras diretamente através dos dados empregados como entrada do modelo. Dessa maneira, é viável caracterizar aprendizagem de máquina como a ciência de conceber modelos ou aplicações computacionais capazes de absorver conhecimento diretamente a partir de dados.[59]

Outro ponto que deve ser destacado sobre a lógica da tecnologia em questão é o fato de que muitos programas são desenvolvidos pelos seres humanos de forma que não possam ser aprendidos pelos computadores, no entanto, os computadores adquirem aptidões que os

---

[56] DOMINGOS, Pedro. *O algoritmo mestre:* como a busca pelo algoritmo de *machine learning* definitivo recriará nosso mundo. São Paulo: Novatec, 2017. p. 24.
[57] *Ibidem,* p. 27-28.
[58] VALLIM, Marco Vinicius Bhering de Aguiar. *Inteligência Artificial Explicável Aplicada a Hemogramas como Suporte à Tomada de Decisão em Diagnósticos de COVID-19.* 2021. 99 f. Dissertação (Mestrado) - Curso de Mestrado em Engenharia Elétrica e Computação, Programa de Pós-graduação em Engenharia Elétrica e Computação, Universidade Presbiteriana Mackenzie, São Paulo, 2021. p. 8.
[59] VALLIM, Marco Vinicius Bhering de Aguiar. *Inteligência Artificial Explicável Aplicada a Hemogramas como Suporte à Tomada de Decisão em Diagnósticos de COVID-19*. 2021. 99 f. Dissertação (Mestrado) - Curso de Mestrado em Engenharia Elétrica e Computação, Programa de Pós-graduação em Engenharia Elétrica e Computação, Universidade Presbiteriana Mackenzie, São Paulo, 2021. p. 8-9.

humanos não são capazes de programar. Isto se deve ao fato de existirem diversos tipos de conhecimento e dentre eles habilidades que estão alocadas no subconsciente humano.[60]

Assim, algoritmos de "*machine learning*" "[...] não são programados para resolver problemas específicos, mas para aprender a resolver problemas".[61] Para Tutt, é necessário considerar o potencial de falha de tais algoritmos, especialmente se utilizados de maneira definitiva, isto é, desconsiderando a possibilidade de erro. Esta é uma das maiores preocupações hoje envolvendo o tema inteligência artificial.

A implementação efetiva do aprendizado de máquina envolve a existência de determinadas aplicabilidades, dentre elas, o reconhecimento de fala e imagem, processamento de linguagem natural (NLP – "*natural language processing*"), análises preditivas, e "*deep learning*", área que permite aos computadores que "vejam" e "distingam" objetos e textos em imagens e vídeos.[62]

O processo de aprendizado de sistemas de computação neural é mutável e auto adaptativo, uma vez que os elementos de processamento têm capacidade de se autoajustarem. Nesse sentido, "[...] aprendizado é a auto adaptação ao nível de elemento de processamento".[63] No referido processo, as ligações ponderadas são reguladas para descobrir resultados específicos.

A condição de o aprendizado de máquina ser supervisionado ou não é o que determina a classificação de seus dois subconjuntos. Métodos de aprendizagem são estratégias de modificação dos valores algorítmicos, visando alcançar um padrão de processamento almejado. As técnicas de aprendizado podem ser divididas em: preditivas e descritivas.

O método preditivo atua de forma que dados de treinamento rotulados são inseridos no modelo para que em razão de seu rótulo possam induzi-lo a gerar um resultado esperado. Modelos preditivos seguem a perspectiva do denominado aprendizado supervisionado.[64]

No aprendizado supervisionado, "[...] um supervisor externo fornece ao algoritmo a saída desejada em relação a um padrão de entrada, com isso, é possível comparar a saída do

---

[60] DOMINGOS, Pedro. *O algoritmo mestre:* como a busca pelo algoritmo de *machine learning* definitivo recriará nosso mundo. São Paulo: Novatec, 2017. p. 27-28.

[61] TUTT, Andrew. An FDA for algorithms. *Administrative Law Review*, volume 69, nº 1, P. 85, 2017. Disponível em: https://static1.squarespace.com/static/603ab50ab81d5532a0a4a42b/t/63cc0b15bd14d66a8db3d1c5/1674316568048/R_69-1-Andrew-Tutt.pdf. Acesso em: 10 abr. 2023.

[62] ABRUSIO, Juliana. *Proteção de dados na cultura do algoritmo.* Belo Horizonte: D'Plácido, 2020. p. 91.

[63] LIMA, Isaías. *Inteligência Artificial.* São Paulo: Grupo GEN, 2014. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788595152724/. Acesso em: 09 abr. 2023. p. 53.

[64] FACELI, Katti; LORENA, Ana C.; GAMA, João; *et al*. *Inteligência Artificial* - Uma Abordagem de Aprendizado de Máquina. São Paulo: Grupo GEN, 2021. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788521637509/. Acesso em: 09 mai. 2023. p. 3.

algoritmo com a saída desejada"[65], e em caso de resultados distintos encontrar o erro no modelo. A partir disso, a fórmula do procedimento é regulada a fim de reduzir a discrepância. Pequenos ajustes são efetuados a cada resultado.

O referido método é usualmente utilizado na modelagem de processos. De forma que sua implementação pode ser "*on-line*" ou "*off-line*". No último caso, as informações contidas no conjunto de treinamento permanecem estáticas, e caso haja necessidade de incorporar novos dados, será preciso criar um conjunto destes para o treinamento, que conterá tanto os dados novos quanto antigos.[66]

Dentro do aprendizado descritivo, ao invés de predizer um valor, o modelo identifica regularidades a partir das previsões obtidas por um conjunto de dados. Neste caso, seguem a lógica do aprendizado não supervisionado.[67] Na referida lógica, como o nome antecipa, não há a figura de um supervisor do processo, portanto, a rede neural artificial (também conhecida como "*deep learning*") vai buscar "[...] algum tipo de correlação ou redundância nos dados de entrada".[68]

Dentre as principais tarefas desse método estão o agrupamento de dados e/ou busca de grupos de objetos similares entre si no conjunto de dados. Além disso, também é possível que colabore para encontrar regras de associação, isto é, relacionar os valores do subconjunto de atributos preditivos a valores de outro subconjunto.[69]

Por redes neurais artificiais podemos compreender "[...] modelos computacionais com capacidades de adaptar, aprender, generalizar, agrupar ou organizar dados, nos quais a estrutura operacional é baseada em processamento paralelo."[70] Tal tecnologia foi mencionada anteriormente, pois foi utilizada na criação do modelo eletrônico de Frank Rosenblatt chamado Mark I Perceptron.

---

[65] FLECK, Leandro *et al*. Redes neurais artificiais: Princípios básicos. *Revista Eletrônica Científica Inovação e Tecnologia*, volume 1, nº 13, P. 47-57, 2016. p. 5. Disponível em: http://dx.doi.org/10.3895/recit.v7i15.4330. Acesso em: 11 mai. 2023.

[66] EYNG, Eduardo; SILVA, Flávio Vasconcelos da; PALð, Fernando; FILETI, Ana Maria Frattini. Neural network based control of an absorption column in the process of bioethanol production. *Brazilian Archives Of Biology And Technology*, volume 52, nº 4, P. 961-972, agosto de 2009. FapUNIFESP (SciELO). Disponível em: http://dx.doi.org/10.1590/s1516-89132009000400020. Acesso em: 11 mai. 2023. p. 971.

[67] FACELI, Katti; LORENA, Ana C.; GAMA, João *et al*. *Inteligência Artificial* - Uma Abordagem de Aprendizado de Máquina**.** São Paulo: Grupo GEN, 2021. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788521637509/. Acesso em: 09 mai. 2023. p. 3.

[68] FLECK, Leandro et al. Redes neurais artificiais: Princípios básicos. *Revista Eletrônica Científica Inovação e Tecnologia*, volume 1, nº 13, p. 47-57, 2016, p. 6. Disponível em: http://dx.doi.org/10.3895/recit.v7i15.4330. Acesso em: 11 mai. 2023.

[69] FACELI, Katti; LORENA, Ana C.; GAMA, João *et al*. *Inteligência Artificial* - Uma Abordagem de Aprendizado de Máquina. São Paulo: Grupo GEN, 2021. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788521637509/. Acesso em: 09 mai. 2023. p. 3.

[70] LIMA, Isaías. *Inteligência Artificial.* São Paulo: Grupo GEN, 2014. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788595152724/. Acesso em: 09 abr. 2023. p. 46.

Após o modelo mencionado, outros pesquisadores passaram a se dedicar ao tema, em 1969, Marvin Minsky e Seymor Papert publicaram um livro chamado *Perceptrons*, em que discutem o exemplar criado em 1957 e concluem que este possuía um algoritmo de treinamento básico. Os estudos do tema foram deixados de lado pela maioria dos cientistas e retomados apenas muitos anos depois.

As redes neurais apresentam estruturas arquitetônicas compostas por módulos similares uns aos outros, que realizam o processamento de maneira simultânea. Estas unidades básicas se comunicam enviando informações entre si por meio de conexões. O componente essencial do modelo em questão são as unidades de processamento, também denominadas nós. Este elemento pode ser definido como "[...] modelo matemático que possui inspiração no modelo biológico de um neurônio".[71]

O modelo de neurônio artificial possui uma anatomia correspondente ao humano. Este dispõe de diversos fios de entrada onde são inseridas informações que terão valores atribuídos para serem multiplicadas e posteriormente conectadas entre si por meio de um nó - momento que tais informações são somadas. Caso a informação exceda um certo limiar definido por cálculo matemático, é gerada uma resposta de saída. Este limite pode variar ao depender do modelo.

O protótipo descrito acima foi um dos primeiros a ser desenvolvido, tendo, portanto, uma estrutura mais simplificada. O formato mais utilizado hoje chama-se RNA – Modelo de Rede Neural Artificial. Sua estrutura física é similar ao primeiro, entretanto, os seus componentes são distribuídos em camadas, onde cada elemento fará conexões com os demais. Essas ligações podem assumir distintas disposições, conforme a finalidade almejada.

A mencionada distribuição em camadas também pode ser chamada de rede neural profunda, conforme mencionado previamente ao comentar a criação do projeto "Alexnet" em 2012. A descoberta foi revolucionária, pois permitiu uma conexão organizada entre os neurônios, de maneira a otimizá-los para que pudessem gerar resultados mais precisos, uma vez que cada camada figura como uma instância de tomada de decisão.

A habilidade de processamento de uma rede neural reside nas conexões entre os elementos processadores. Nos valores atribuídos para cada conexão estão depositadas as informações aprendidas pela rede. Das associações e ligações entre estes elementos surgem

---

[71] *Ibidem*, p. 47.

novas estruturas. “Em uma RNA os neurônios podem estar agrupados por camadas direcionadas ou não, com ligações em um sentido (para frente), em outro (para trás) ou em ambos”.[72]

Não obstante os diversos frutos trazidos pela ascensão do “*deep learning*”, a profundidade da estrutura de seus algoritmos desafia ainda mais a transparência.[73] Tal crítica é realizada quando a estrutura do algoritmo ou rede neural não é revelada de maneira satisfatória. Entretanto, como mencionado por Turing inicialmente, em muitos casos o programador não tem controle dos caminhos e conexões que serão formadas após inserir as informações em uma rede não supervisionada.

Ainda, fundamental relembrar que “[...] os algoritmos de aprendizado de máquina não aprendem nem raciocinam como os humanos, e isso pode dificultar a previsão e a dificuldade de explicar seus resultados”.[74] A autora afirma, na sequência, que a implicação disto é que em algumas das aplicações mais cruciais para as quais os algoritmos poderiam ser utilizados no futuro estaríamos confiando o destino dos seres humanos a máquinas desconhecidas e possivelmente incompreensíveis.

Para Abrusio, os algoritmos que impulsionam a inteligência artificial atual podem ser equiparados à entropia, princípio da física termodinâmica, uma vez que modificam o estado de organização de seus comandos iniciais, gerando novas condições em seus sistemas de maneira irreversível, em um processo de des(organização).[75] Nesse sentido, Andrew Selbt e Julia Powles[76] postulam que entre as diversas opções de tomada de decisão, os sistemas de aprendizado de máquina e inteligência artificial são os únicos capazes de desafiar completamente a compreensão humana, representando um risco potencial.

Complementam Bryce Goodman e Seth Flaxman[77], de maneira a se dirigir aos obstáculos técnicos que se contrapõem à explicação dos algoritmos de “*machine learnig*”, de acordo com os autores, tal tecnologia de fato torna esse tipo de algoritmo um modelo opaco. Além disso, chamam a atenção para o paradoxo entre a capacidade de representação de um

---

[72] LIMA, Isaías. *Inteligência Artificial.* São Paulo: Grupo GEN, 2014. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788595152724/. Acesso em: 09 abr. 2023. p. 52.

[73] SINGH, Jatinder; WALDEN, Ian; CROWCROFT, Jon; BACON, Jean. Responsibility & Machine Learning: part of a process. *Ssrn Electronic Journal*, 2016. Elsevier BV. Disponível em: http://dx.doi.org/10.2139/ssrn.2860048. Acesso em: 10 abr. 2023.

[74] ABRUSIO, Juliana. *Proteção de dados na cultura do algoritmo.* Belo Horizonte: D’Plácido, 2020. P. 94.

[75] *Ibidem*. p. 95.

[76] SELBST, Andrew; D. POWLES, Julia, Meaningful Information and the Right to Explanation. *International Data Privacy Law*, volume 7, nº 4, 2017. p. 233-242. Disponível em: https://ssrn.com/abstract=3039125. Acesso em: 11 abr. 2023. p. 234.

[77] GOODMAN, Bryce.; FLAXMAN, Seth. European Union Regulations on Algorithmic Decision-Making and a “Right to Explanation”. *AI Magazine*, Volume 38, nº 3, 2017. p. 50-57. Disponível em: https://doi.org/10.1609/aimag.v38i3.2741. Acesso em: 11 abr. 2023. p. 55.

modelo e sua compreensão pelos humanos, impasse esse que já foi abordado previamente no texto.

Em razão das considerações mencionadas, surge um clamor em torno do que se denominou transparência algorítmica e o direito à explicação. Tais questionamentos não surgiram especificamente pelos avanços da inteligência artificial, mas sim do próprio processamento de dados, de modo que foram positivados em diferentes diplomas legais como a Lei Geral de Proteção de Dados no Brasil[78] e a chamada GDPR – *General Data Protection Regulation*[79] na União Europeia.

O princípio da inteligência artificial explicável (XAI – "*Explainable artificial intelligence*") surge como resposta a esses temores. Este pode ser definida como o conjunto de novas técnicas ou técnicas modificadas de aprendizado de máquina que produzam modelos mais transparentes, que possam ser devidamente compreendidos pelos usuários finais ao serem combinados com técnicas eficazes de esclarecimento, permitindo que estes saibam como confiar e gerenciar adequadamente a ascensão de sistemas em desenvolvimento de inteligência artificial.[80]

Para o referido princípio, a presença do atributo da transparência deve ser um elemento fundamental nos sistemas inteligentes, transmitindo segurança ao usuário. Além disso, é crucial que os sistemas de inteligência artificial, sobretudo aqueles que apresentam riscos elevados, sejam considerados confiáveis.

Entretanto, para Sandra Wachter, Brent Mittelstad e Luciano Floridi[81], a própria efetivação de tais direitos é uma ideia complexa, dar o próximo passo e trazer estes conceitos para o mundo do "*machine learning*" pode ser ainda mais complicado do que parece. Explicam,

---

[78] Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.
Ainda, a referida lei também prevê o direito do titular de dados à explicação, conforme artigo a seguir: Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso.

[79] Art. 12 - Transparência das informações, das comunicações e das regras para exercício dos direitos dos titulares dos dados: O responsável pelo tratamento toma as medidas adequadas para fornecer ao titular as informações a que se referem os artigos 13 e 14 e qualquer comunicação prevista nos artigos 15 a 22 e 34 a respeito do tratamento, de forma concisa, transparente, inteligível e de fácil acesso, utilizando uma linguagem clara e simples, em especial quando as informações são dirigidas especificamente a crianças. As informações são prestadas por escrito ou por outros meios, incluindo, se for caso disso, por meios eletrônicos. Se o titular dos dados o solicitar, a informação pode ser prestada oralmente, desde que a identidade do titular seja comprovada por outros meios.

[80] TUREK, Matt. *Defense Advanced Research Project Agengy (DARPA).* Disponível em: https://www.darpa.mil/program/explainable-artificial-intelligence. Acesso em: 11 abr. 2023.

[81] WACHTER, Sandra; MITTELSTADT, Brent; FLORIDI, Luciano. Why a right to explanation of automated decision-making does not exist in the general data protection regulation. *International Data Privacy Law*, volume 7, nº 2, P. 76-99, 2017. Disponível em: https://ssrn.com/abstract=2903469. Acesso em: 11 abr. 2023. p. 80.

o reconhecimento de um direito à explicação implica que os controladores[82] de dados tenham plena compreensão de quais obrigações precisam ser cumpridas, de maneira que os punir por negligência em relação a essas obrigações, sem a adequada explanação entra em conflito com os princípios de um julgamento justo.

Nessa linha, para Andrew Selbst e Julia Powles,[83] o direito à explicação deve ser interpretado de forma funcional e adaptável, permitindo que o proprietário dos dados possa exercê-lo de diversas maneiras, sendo a utilidade o fator empregado para determinar o que seria uma explicação satisfatória. Os autores, entretanto, adotam a premissa de que se as aplicações de um sistema podem ser explicadas, também podem as motivações de um algoritmo.

Em que pese as considerações dos autores tenham consistência, acreditamos que o princípio em questão não foi idealizado considerando que aquele que o invocasse teria como base conhecimentos técnicos avançados de programação algorítmica, de forma que foi pensado para o usuário comum. Quanto às reflexões acerca do conhecimento das obrigações por parte dos controladores, acreditamos que a alteração legal, ou, no caso da inteligência artificial, regulação, não serão suficientes se não forem pautadas por princípios éticos que deverão resultar uma verdadeira cultura de proteção de dados e inteligência artificial ética.

Os modelos que demonstram superioridade em análises classificatórias e preditivas são precisamente aqueles que se revelam mais desafiadores de serem interpretados. Essa problemática é sensível, pois confiar decisões críticas a sistemas que não conseguem se explicar por si mesmos pode acarretar um nível elevado de risco, dada a natureza crítica das decisões a serem realizadas. É fundamental compreender que os modelos de inteligência artificial devem atender a alguns critérios que funcionam como garantias para fortalecer a confiança neles, incluindo imparcialidade, confiabilidade, segurança, justificabilidade explicativa, privacidade, usabilidade, entre outros.

Ao abordar a urgência de fornecer explicações para a realização de uma decisão, frequentemente se refere à necessidade de motivos e fundamentos para aquela decisão específica, não à descrição dos cálculos internos ou à lógica empregada por trás do processo decisório. Sistemas de Explicabilidade em Inteligência Artificial (XAI), obrigatoriamente, devem disponibilizar as informações indispensáveis para justificar suas operações,

---

[82] Por controlador de dados adotamos o conceito legal da LGPD: Art. 5º Para os fins desta Lei, considera-se: VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

[83] SELBST, Andrew D. POWLES, Julia, Meaningful Information and the Right to Explanation. International Data Privacy Law, volume 7, nº 4, 2017. P. 233-242. Disponível em: https://ssrn.com/abstract=3039125. Acesso em: 11 abr. 2023. p. 242.

especialmente quando decisões imprevistas são efetuadas. A capacidade de elucidar as decisões do modelo não é crucial apenas para justificá-las, mas também para prevenir possíveis falhas. Uma compreensão mais aprofundada sobre o comportamento do sistema auxilia na detecção de vulnerabilidades ou falhas, possibilitando a correção desses equívocos ou a realização de ações de depuração, o que resulta em um maior controle sobre o sistema.[84]

O autor sustenta que, a despeito de ser uma característica crucial, a compreensibilidade de um modelo nem sempre é imprescindível. Exigir que todos os sistemas de inteligência artificial sejam capazes de oferecer explicações para cada uma de suas decisões pode resultar, de fato, em sistemas menos eficazes. Sistemas elucidativos requerem recursos, tanto computacionais quanto da equipe de desenvolvimento.

Portanto, é essencial determinar quando e por que é necessário prover tais esclarecimentos, pois eles dependem do nível de opacidade funcional resultante da complexidade dos algoritmos e da capacidade do sistema de tolerar erros. Se estivermos lidando com um sistema destinado à publicidade direcionada, por exemplo, um grau reduzido de interpretabilidade é suficiente, ao contrário de um sistema de IA voltado para realizar diagnósticos médicos, no qual os erros acarretam custos muito mais elevados devido à natureza crítica inerente à área da saúde e à medicina diagnóstica.[85]

A dicotomia entre a necessidade de compreensibilidade e os desafios apresentados por modelos altamente eficazes em análises classificatórias e preditivas se faz novamente presente neste momento, entretanto, a sensibilidade da situação é salientada ao ressaltar o risco inerente a confiar decisões críticas a sistemas de IA que não conseguem fornecer explicações claras para suas escolhas.

A necessidade de transparência nas operações do modelo, especialmente quando decisões inesperadas são tomadas, é mais uma vez destacada, juntamente com a tão defendida aqui necessidade de equilíbrio. De forma que os cenários em que está inserida a IA, assim como seu grau de opacidade, devem ser considerados para definir os critérios de transparência e explicabilidade.

Podemos observar uma perspectiva abrangente sobre os desafios e considerações cruciais relacionados à interpretabilidade de modelos de inteligência artificial, enfatizando a

---

[84] VALLIM, Marco Vinicius Bhering de Aguiar. *Inteligência Artficial Explicável Aplicada a Hemogramas como Suporte à Tomada de Decisão em Diagnósticos de COVID-19.* 2021. 99 f. Dissertação (Mestrado) - Curso de Mestrado em Engenharia Elétrica e Computação, Programa de Pós-Graduação em Engenharia Elétrica e Computação, Universidade Presbiteriana Mackenzie, São Paulo, 2021. p. 9-11.
[85] *Ibidem*.

importância de critérios específicos e uma abordagem contextualizada para determinar o nível apropriado de compreensibilidade em diferentes contextos.

Ao longo deste capítulo discutimos os primórdios da inteligência artificial, isto é, desde a visão de Turing sobre o assunto e a criação de seu teste, ideias contrapostas posteriormente por Searle e o teste sugerido por ele, até passarmos por um panorama relacionado aos principais acontecimentos sobre o tema. As visões de autores como John McCarthy, um dos pesquisadores responsáveis por denominar a referida tecnologia, também foram apresentadas, assim como feitos mais recentes da inteligência artificial em diversas áreas e os conflitos em razão disto.

Na segunda parte, foi construído o conceito sobre o tema que será adotado neste trabalho, assim como abordado o assunto iniciado e tão debatido no ponto anterior, aprendizado de máquina. De modo que discutimos o funcionamento das chamadas "*machine learning*" e seu aprofundamento em redes neurais artificiais. Tal divisão buscou abordar conceitos e procedimentos de outros campos da ciência de maneira acessível ao leitor jurista, para que este pudesse ter uma compreensão da parte técnica dos pontos aqui examinados, sendo possível visualizar os problemas em diversas faces e contribuir na construção de debates ainda mais interdisciplinares.

Por fim, ao longo deste capítulo foi se tornando cada vez mais evidente o papel destacado que os dados utilizados em qualquer aplicação de inteligência artificial têm, de forma que sua proteção e qualidade podem influenciar demasiadamente o funcionamento e resultados do tema em questão. Podemos concluir que a inteligência artificial será tão boa quanto a qualidade de seus dados. Este assunto será abordado no próximo capítulo com mais profundidade.

2. PROTEÇÃO DE DADOS NA ERA DA INTELIGÊNCIA ARTIFICIAL: DESAFIOS E PERSPECTIVAS

2.1 A PROTEÇÃO DE DADOS COMO UM DIREITO FUNDAMENTAL

Quando falamos sobre proteção de dados, no Brasil, é comum que a primeira associação seja com a Lei Geral de Proteção de Dados, entretanto, a referida lei é fruto de progressivas reinvindicações acerca de tais direitos, além disso, ainda que estes tenham sido finalmente positivados em um diploma legal específico, não podemos deixar de lado o período em que esteve atrelado ao direito de privacidade. Tal período demonstra que, embora a proteção de dados não estivesse mencionada expressamente, as preocupações quanto ao tema já estavam presentes desde os debates iniciais.

Contudo, antes de adentrarmos as discussões sobre estes assuntos e suas relações com a inteligência artificial, necessário definir o que é um dado e uma informação. Os termos em questão são usualmente utilizados como sinônimos, porém, para Danilo Doneda, são bem distintos. O autor define dado como informação em estado potencial, isto é, anterior a um processo de elaboração, já a informação pode ser indicada como algo além da representação contida no dado. Neste caso, já se pressupõe a depuração de seu conteúdo.[86]

O autor prossegue seu raciocínio afirmando que o que destaca a informação de seu significado anterior é a maior desenvoltura de sua manipulação, desde sua coleta e tratamento a sua comunicação. A variável que estabelece essa distinção é exatamente a tecnológica ao ampliar a habilidade de armazenamento e comunicação, expande também a diversidade de maneiras pelas quais os dados podem ser adquiridos ou empregados.

Ainda que a distinção do autor seja de extrema relevância para este trabalho, adotaremos o conceito legal de dado, estabelecido pela LGPD em seu artigo 5º, inciso I[87], pois consideramos sua amplitude mais adequada às reflexões aqui propostas, da mesma forma, em relação aos dados sensíveis.

No contexto jurídico, esse crescente significado se manifesta no sentido de que uma considerável porção das prerrogativas pessoais atualmente são efetivadas em estruturas ou

---

[86] DONEDA, Danilo. *Da Privacidade à Proteção de Dados Pessoais:* Fundamentos da Lei Geral de Proteção de Dados. 3ª edição, São Paulo: Thomson Reuters Brasil, 2021. p. 140.

[87] Art. 5º Para os fins desta Lei, considera-se:
I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

plataformas onde a comunicação e a informação desempenham um papel importante. Trazendo à tona debates sobre a propriedade dos meios de comunicação, liberdade de informação, de expressão e de imprensa, assim como a caracterização da informação como um bem jurídico e até mesmo a propriedade intelectual.[88]

No âmbito do direito civil, em particular, uma das opções viáveis seria a validação da essência jurídica da informação e, a partir disso, a utilização dos mecanismos do direito de propriedade para organizar o assunto. O fato de a informação não possuir um valor intrínseco visível não impede o estabelecimento de estruturas que o concretizem.

Tal visão já foi adotada por Lawrence Lessig, em 2002, em relação à privacidade. No texto *Privacy as property*[89] o autor discorre sobre aspectos culturais que apoiam os valores da privacidade e para ele tais direitos seriam mais bem aceitos pela sociedade norte americana em que está inserido, caso falássemos deles como uma forma de propriedade.

Apesar de ter consciência que tal visão não é unânime entre os pesquisadores do tema, o autor argumenta ser uma alternativa viável, pois a privacidade, assim como a propriedade física, é um recurso escasso. Para o autor, as pessoas devem ter o direito de controlar e gerenciar suas informações pessoais, podendo decidir como e quando compartilhá-las. A alternativa proposta por Lessig poderia ter sido adotada como estratégia quando foi produzida, entretanto, não foram estes caminhos os tomados pela proteção da privacidade.

A ideia de privacidade, em sua essência, não é nova, com as várias interpretações que podem ser adotadas. No entanto, passou a ser efetivamente tratada pela legislação apenas no final do século XIX, para então assumir suas características atuais. A doutrina moderna da proteção do direito à privacidade teve início com o artigo de Warren e Brandeis, *The right to privacy*.[90]

Esta foi marcada desde o princípio por um individualismo exacerbado, do direito a ser deixado só, ou uma ausência de comunicação entre uma pessoa e as demais. Após muitos anos houve uma crescente conscientização de que a privacidade poderia se configurar como um aspecto fundamental da realização da pessoa e do desenvolvimento de sua personalidade.[91]

---

[88] DONEDA, Danilo. *Da Privacidade à Proteção de Dados Pessoais:* Fundamentos da Lei Geral de Proteção de Dados. 3ª edição, São Paulo: Thomson Reuters Brasil, 2021. p. 141.
[89] LESSIG, Lawrence. Privacy as Property. *The Johns Hopkins University Press*, Baltimore, volume 69, nº 1, p. 247-269, setembro de 2002. Disponível em: https://www.jstor.org/stable/40971547. Acesso em: 15 abr. 2023.
[90] WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. *Harvard Law Review*, volume 4, nº 5, p. 193, dezembro de 1890. Disponível em: http://dx.doi.org/10.2307/1321160. Acesso em: 15 abr. 2023.
[91] DONEDA, Danilo. *Da Privacidade à Proteção de Dados Pessoais*: Fundamentos da Lei Geral de Proteção de Dados. 3ª edição, São Paulo: Thomson Reuters Brasil, 2021. p. 30.

Hoje, o conceito abrange questões muito mais complexas que a ideia inicial de isolamento e tranquilidade.

A ideia mencionada permaneceu desde o momento em que tal direito passou a ser inserido em ordenamentos jurídicos, até a década de 1960. Quando a ideia de um estado de bem-estar social aumentou consideravelmente o fluxo de informações, tal momento condiz com os crescentes desenvolvimentos tecnológicos mencionados no capítulo anterior. Com o passar dos anos, a capacidade de coleta, processamento e utilização das informações foi altamente ampliada.

Simultaneamente, a importância da informação também aumentou, de forma que não eram mais apenas figuras de grande relevo social que poderiam ter sua privacidade violada. Neste momento podemos estabelecer dois fatores que com frequência figuram dentre as justificativas para a utilização de informações pessoais: a eficiência e o controle.[92]

Para Doneda, o primeiro ente a utilizar largamente informações pessoais foi o Estado. Sob os motivos mencionados previamente, neste caso, uma administração pública mais eficiente. Já em relação ao controle, diversas formas de exercê-lo poderiam seriam ser potencializadas com uma coleta e armazenamento de dados[93] significativos, aumentando seu poder sobre os cidadãos. Para o autor, a razão de acontecimento se dá pela desproporção de capacidade computacional entre o Estado e organismos privados.

Estes, inicialmente, não enxergavam a atividade em questão como um meio atraente de investimentos. Entretanto, como sabemos, a partir do momento que a tecnologia possibilitou tal coleta e processamento reduzindo os custos de e oferecendo uma série extensa de possibilidades de utilização, a barreira mencionada ruiu. Finalmente, o autor afirma que "[...] a tecnologia, em conjunto com as mudanças ocorridas no tecido social, vai definir diretamente o contexto no qual a informação pessoal e a privacidade atualmente se relacionam".[94]

Nesse sentido, Abrusio argumenta, na era da sociedade de dados, em que nossas informações estão constantemente em circulação, o direito de gerenciar a forma como terceiros utilizarão esses dados tornou-se indispensável, principalmente considerando que a coleta e o processamento desses podem resultar em discriminação ou estigmatização social.[95] Em artigo

---

[92] DONEDA, Danilo. *Da Privacidade à Proteção de Dados Pessoais:* Fundamentos da Lei Geral de Proteção de Dados. 3ª edição, São Paulo: Thomson Reuters Brasil, 2021. p. 33.

[93] Em que pese a precisa distinção terminológica entre "dado" e "informação", os utilizaremos como sinônimos no decorrer do presente trabalho para facilitar seu andamento e compreensão. Uma vez que, assim também é o comportamento de grande parcela dos pesquisadores do tema e não consideramos que tal ato resulte em prejuízos.

[94] DONEDA, Danilo. *Da Privacidade à Proteção de Dados Pessoais:* Fundamentos da Lei Geral de Proteção de Dados. 3ª edição, São Paulo: Thomson Reuters Brasil, 2021. p. 35.

[95] ABRUSIO, Juliana. *Proteção de dados na cultura do algoritmo.* Belo Horizonte: D'Plácido, 2020. p. 127.

de 1987, Spiros Simitis aponta que o aumento da capacidade de processamento de dados teve três consequências:

1) Os problemas relacionados à privacidade não possuem mais uma origem individualista, mas destacam situações que afetam a grandes grupos de pessoas; 2) A vigilância perdeu sua natureza excepcional e se transformou em uma prática cada vez mais frequente; 3) Os dados pessoais são cada vez mais utilizados para impor normas de conduta.[96]

Em relação à vigilância, a abordaremos na segunda parte deste item, neste momento vamos nos direcionar para o argumento número três. No Brasil, a proteção de dados pessoais alcançou não apenas "status" constitucional, mas foi incluída no rol de direitos e garantias fundamentais no ano de 2022.[97]

Para Carlos Alberto Bittar, os direitos da personalidade figuram como direitos inatos, cabendo ao Estado apenas o reconhecimento e a positivação (em nível constitucional ou não). Caso a opção escolhida seja a constitucional, além de serem transformados em direitos fundamentais, sua consideração e enfoque no plano positivo e passam a contar com todo o sistema de proteção que lhe é próprio.[98]

Como mencionado acima, este foi o caso brasileiro. Em seu artigo *Autodeterminação informativa: a história de um conceito*, Laura Schertel Mendes discorre sobre a jornada alemã acerca do reconhecimento do chamado direito geral de personalidade. Este representaria um direito de liberdade indefinido, que complementaria os direitos específicos.[99]

Tendo em vista que os avanços contemporâneos podem acarretar novos riscos para o indivíduo, isso representaria um grande desafio para a proteção da personalidade na atualidade. Logo, "[...] o direito geral de personalidade serviria para conceder proteção por meio de sua formulação abstrata contra riscos ainda desconhecidos e imprevisíveis". Para o Tribunal Constitucional Alemão, não seria viável a delimitação de maneira definitiva do teor desse

---

[96] SIMITIS, Spiros. Reviewing Privacy in an Information Society. *University Of Pennsylvania Law Review*, volume 135, nº 3, p. 707-746, março de 1987. Disponível em: http://dx.doi.org/10.2307/3312079. Acesso em: 15 abr. 2023. p. 709-710.

[97] Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.

[98] BITTAR, Carlos Alberto. *Os direitos da personalidade.* 8ª edição. São Paulo: Saraiva, 2015. p. 38-39.

[99] MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a história de um conceito. *Pensar-Revista de Ciências Jurídicas*, volume 25, nº 4, 2020. p. 8-9. Disponível em: https://doi.org/10.5020/2317-2150.2020.10828. Acesso em: 3 jun. 2023.

direito, pois, na realidade, diversos conceitos foram elaborados por meio de construção jurisprudencial.[100]

As concepções delineadas nos conduzem a uma perspectiva fundamentada em princípios, respeitando as devidas proporções, é claro. Nesse sentido, ressaltam a importância de considerar a ideia de direitos ou regulamentações abrangentes, que sejam complementares e sirvam como orientação, sem impor limites inflexíveis. Além disso, sublinham a necessidade de um enfoque mais flexível e adaptável, capaz de acompanhar a dinâmica das transformações sociais e tecnológicas.

Tal raciocínio se encaminha para o mencionado anteriormente de que uma regulamentação de inteligência artificial deveria buscar uma harmonia com os diplomas legais já existentes. Além disso, considerando o momento em que se encontra a tecnologia, tal normativa teria maior aderência com a realidade se elegesse a via principiológica.

Os diálogos que permearam a discussão sobre a regulação da proteção de dados eventualmente se repercutem nos debates cujo tema é a regulação da inteligência artificial. Tal efeito se dá, pois além da familiaridade dos temas com a tecnologia, eles estão efetivamente ligados, uma vez que não há inteligência artificial sem dados, sendo a ideia deste capítulo, justamente, explorar estas conexões e suas consequências.

Após a digressão acima retornaremos à classificação da proteção de dados como direito fundamental. Nesse sentido, Bruno Bioni "[...] as atividades de processamento de dados têm ingerência na vida das pessoas. Hoje vivemos em uma sociedade e uma economia que se orientam e movimentam a partir desses signos identificadores do cidadão".[101] Continua, "[...] para além da perspectiva subjetiva de que cada ser humano detém seus prolongamentos – atributos e características próprias que o tornam singular –, encaixam-se os dados pessoais como um elemento que compõe essa singularidade".[102]

Para o autor mencionado, os dados pessoais se caracterizam como um prolongamento da pessoa e são instrumentais para que tal pessoa possa livremente desenvolver sua personalidade.

Ademais, André de Carvalho Ramos postula que existem duas formas de analisar o direito à proteção de dados. A perspectiva subjetiva garante a proteção do indivíduo contra a

---

[100] MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a história de um conceito. *Pensar-Revista de Ciências Jurídicas*, volume 25, nº 4, 2020. p. 8-9. Disponível em: https://doi.org/10.5020/2317-2150.2020.10828. Acesso em: 3 jun. 2023.

[101] BIONI, Bruno R. *Proteção de Dados Pessoais:* A Função e os Limites do Consentimento. 3ª edição. Rio de Janeiro: Forense, 2021, p. 57.

[102] *Ibidem*.

utilização indevida da coleta, tratamento, utilização e circulação das informações pessoais; na perspectiva objetiva, exige-se o compromisso do Estado em assegurar o domínio do fluxo das informações pessoais, garantindo a autonomia informacional por parte do indivíduo.[103]

Nesse sentido, o autor também menciona as diferentes interpretações sobre o referido direito, tais como: direito autônomo e direito derivado da proteção à privacidade. No primeiro caso, teria surgido da era digital, na qual existe uma ampla capacidade de guardar, processar, transmitir e obter acesso aos dados, o que levou o legislador a estabelecer o direito na lista dos direitos fundamentais e criar leis e estabelecer instituições administrativas.[104]

Já no segundo, teria sido extraído da previsão constitucional em seu artigo 5º, inciso X. Conforme mencionado previamente, o autor também afirma que no plano infraconstitucional a proteção de dados já era refletida no âmbito da privacidade e foi estabelecida em leis setoriais.

Desse modo, para Paulo Bonavides, são direitos de quarta geração o direito à democracia, o direito à informação e o direito ao pluralismo. Deles decorre a realização da sociedade aberta para o futuro, em sua amplitude máxima, para a qual o mundo parece se predispor em todas as interações sociais.[105]

Os entendimentos mencionados foram adotados similarmente pela relatoria do Projeto de Emenda Constitucional número 17 de 2019 (que resultou na Emenda Constitucional número 115 de 2022). Em parecer apresentado em 22 de maio de 2019, a senadora Simone Tebet afirmou que questões concretas e contemporâneas, como a aplicabilidade direta dos direitos fundamentais, a salvaguarda dos direitos individuais, especialmente a preservação da privacidade e intimidade, o direito ao esquecimento como componente relacionado aos direitos individuais, trazem à tona a urgência de proteger as informações pessoais com uma abordagem constitucional.[106]

Em abril de 2020, houve a publicação da Medida Provisória 954/2020 com o intuito de facilitar a realização da Pesquisa Nacional por Amostragem de Domicílios (PNAD) pelo IBGE durante o contexto da pandemia, levando em consideração os perigos associados à execução presencial da pesquisa estatística. A alternativa proposta pelo governo consistiu na

---

[103] RAMOS, André de C. *Curso de Direitos Humanos.* 9ª edição. São Paulo: Editora Saraiva, 2022. p. 594. Disponível em: https://app.minhabiblioteca.com.br/#/books/9786553622456/. Acesso em: 11 jun. 2023.
[104] *Ibidem*.
[105] BONAVIDES, Paulo. *Curso de direito constitucional.* 18ª edição. São Paulo: Malheiros, 2006, p. 571.
[106] TEBET, Simone. *Relatório legislativo à comissão de constituição, justiça e cidadania.* Brasília, 2019. p. 5. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=7956536&ts=1647518557553&disposition=inline&_gl=1*1lu93t7*_ga*MTE1ODAxNDMzNy4xNjY2NTc4NTk5*_ga_CW3ZH25XMK*MTY4NjUyNTMxNy42LjAuMTY4NjUyNTMxNy4wLjAuMA. Acesso em: 11 jun. 2023.

aquisição de informações pessoais de usuários de serviços de telecomunicações (linhas fixas e dispositivos móveis) para efetivar a condução remota da pesquisa.

A legalidade da medida foi questionada por cinco Ações Diretas de Inconstitucionalidade.[107] O argumento central era a inconstitucionalidade material da Medida Provisória, devido à violação direta dos arts. 1º, III e 5º, X e XII da Constituição Federal. Na solicitação de medida cautelar, o Conselho Federal da OAB (Ordem dos Advogados do Brasil), cujo processo foi destacado como principal, enfatiza a importância dos direitos constitucionais à autodeterminação informativa, à dignidade da pessoa humana, à privacidade, à intimidade e à salvaguarda de dados.

Em abril de 2020, a Ministra Rosa Weber, na condição de relatora, deferiu a liminar solicitada pela parte demandante,

> [...] para interromper a eficácia da Medida Provisória 954/2020, determinando consequentemente que o Instituto Brasileiro de Geografia e Estatística (IBGE) se abstenha de requerer a disponibilização dos dados objeto da mencionada Medida Provisória e, se já o tiver feito, que cancele tal solicitação, comunicando imediatamente à(s) operadora(s) de telefonia.

O referendo da liminar pelo Plenário foi agendado para o dia 06 de maio de 2020, quando se manifestaram os "*amici curiae*", o Procurador-Geral da República e o Advogado-Geral da União, e a Ministra Rosa Weber reiterou sua posição. No dia seguinte (7), os demais Ministros votaram, resultando em uma votação de 10x1 a favor da confirmação da liminar para suspender a eficácia da Medida Provisória. O voto dissidente foi proferido pelo Ministro Marco Aurélio de Mello.

Estamos diante de uma determinação de grande relevância que reconhece a autonomia inerente ao direito à proteção de dados, classificando-o como um novo direito fundamental. Anteriormente, a Suprema Corte vinha decidindo casos relacionados à proteção de dados com base na perspectiva do direito à privacidade. Ou seja, interpretando que a Constituição protegeria apenas dados confidenciais e a preservação de sua natureza sigilosa.[108]

Como podemos observar a seguir:

> Até então, historicamente, a Suprema Corte vinha decidindo casos sobre proteção de dados pessoais baseando-se na lógica do direito à privacidade. Isto é, considerando que a Constituição tutelaria apenas dados sigilosos e a conservação da sua natureza confidencial. No Recurso Extraordinário 601314,[109] decidiu-se ser lícito o acesso, sem

---

[107] i) ADI 6387 – Conselho Federal da Ordem dos Advogados do Brasil – OAB; ii) ADI 6388 – Partido da Social Democracia Brasileira – PSDB; iii) ADI 6389 – Partido Socialista Brasileiro – PSB; iv) ADI 6390 – pelo Partido Socialismo e Liberdade – PSOL; v) ADI 6393 pelo Partido Comunista do Brasil.

[108] BIONI, Bruno R. *Proteção de Dados Pessoais:* A Função e os Limites do Consentimento. 3ª ed. Rio de Janeiro: Forense, 2021. p. 102-103.

[109] BRASIL, Supremo Tribunal Federal. *Recurso Extraordinário 601314*, Rel. Min. Edson Fachin, Tribunal Pleno, julgado em 24.2.2016, DJe 16.9.2016.

> a necessidade de ordem judicial, por parte da Receita Federal, aos dados de transações financeiras junto aos Bancos. No Recurso Extraordinário 1055941,[110] também considerou-se ser legal a requisição de informações sobre transações financeiras por parte do Ministério Público à Receita Federal. Em ambos os casos, o argumento central foi que tais dados-informações não deixariam de ser sigilosos, uma vez que seriam manipulados em ambiente controlado e, sobretudo por instituições cujos servidores-membros teriam um dever fiduciário em não publicizá-los. Além disso, não seriam dados sensíveis (de alto grau de intimidade) sobre os indivíduos (e.g., religião, orientação político-partidária), o que tornaria proporcional tal tipo de interferência diante do interesse público a ser ponderado, qual seja, o combate a ilícitos.[111]

Um dos pontos fundamentais da decisão foi a declaração de que não existem dados sem importância, seguindo a trilha da decisão pioneira do Tribunal Constitucional alemão sobre a Lei do Censo de 1983.[112] Essa constatação está em desacordo com as posições da Procuradoria-Geral da República e da Advocacia-Geral da União, que argumentaram que os dados compartilhados com o IBGE – como nome, telefone e endereço – eram triviais, simples "dados de lista telefônica" e, portanto, sujeitos à publicidade. De acordo com a Ministra Cármen Lúcia, o contexto em que os dados pessoais poderiam ser reduzidos a essa concepção já não existe mais. A Ministra Relatora Rosa Weber entendeu da mesma maneira.[113]

Essa abordagem acarreta uma implicação significativa: implica afirmar que a Constituição Federal resguarda não apenas os dados confidenciais (conforme o disposto no art. 5º, XII, que protege o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas), mas qualquer dado que, por sua natureza, seja uma característica da individualidade humana. Assim sendo, o novo precedente marca uma reviravolta histórica na jurisprudência do STF, que passa a não restringir a proteção constitucional apenas ao caráter confidencial de uma informação. É suficiente que um dado seja uma propriedade da personalidade – individual – para suscitar a proteção constitucional.[114]

A argumentação acima situa a decisão mencionada em um contexto mais amplo de proteção de dados, referindo-se a casos anteriores em que a Suprema Corte fundamentava suas decisões na perspectiva do direito à privacidade. Essa contextualização destaca a alteração de paradigma ao reconhecer que todos os dados, não apenas os confidenciais, possuem importância e merecem proteção constitucional. O novo precedente, ao estabelecer um marco histórico na

---

[110] BRASIL, Supremo Tribunal Federal. *Recurso Extraordinário 1055941*, Rel. Min. Dias Toffoli, Tribunal Pleno, julgado em 28.11.2019. DJe 6.10.2020.
[111] BIONI, Bruno R. *Proteção de Dados Pessoais:* A Função e os Limites do Consentimento. 3ª ed. Rio de Janeiro: Forense, 2021. p. 103-104.
[112] MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a história de um conceito. *Pensar Revista de Ciências Júridicas Universidade de Fortaleza (Unifor)*, Fortaleza, v. 25, n. 4, p. 1-18, 2020.
[113] BIONI, Bruno R. *Proteção de Dados Pessoais:* A Função e os Limites do Consentimento. 3ª ed. Rio de Janeiro: Forense, 2021. p. 104.
[114] *Ibidem*, p. 104-105.

jurisprudência do STF, amplia a proteção constitucional para além do caráter confidencial, englobando qualquer dado que constitua uma propriedade da personalidade. Essa mudança representa o reconhecimento da importância e autonomia do direito à proteção de dados como um novo direito fundamental.

Até aqui buscamos desenhar brevemente a trajetória do direito a proteção de dados no cenário brasileiro. Os próximos passos serão baseados em analisar as implicações de coletas e usos de dados em nosso cotidiano.

Possivelmente o exemplo mais famoso de utilização massiva de dados seja o caso da "Cambridge Analytica", em que a partir de dados coletados em redes sociais e outras plataformas foram identificados quais usuários estariam mais suscetíveis a tipos específicos de conteúdo e o direcionavam para tal público.[115] Hoje sua metodologia de ação se popularizou e "[...] a oferta de serviços voltados à análise quantitativa de dados de campanha cresceu à medida que a análise preditiva ganhou pontos de apoio em outros setores da economia".[116]

O referido caso tomou grandes proporções por consistir no emprego da tecnologia mencionada para influenciar pleitos eleitorais e discussões políticas ao redor do mundo. Ainda que não seja o foco deste trabalho debater especificamente as possíveis consequências de tais ações nas disputas eleitorais, é inegável que, uma vez se trata de um direito da personalidade e que, portanto, interfere na visão de mundo de uma pessoa, qualquer manipulação deste poderá repercutir em seu comportamento em sociedade e na forma de exercer sua cidadania de diversas formas.

Em 2021, o Instituto Alan Turing publicou um guia denominado *Human rights, democracy and the rule of law assurence framework for AI systems*, que contém uma estratégia para mitigar os riscos envolvendo "*big data*" e inteligência artificial. A proposta consiste em um questionário de setenta e uma questões, para realizar uma análise preliminar de risco baseada em contexto.

A referida análise leva em conta os chamados fatores de risco circunstanciais, tais como os que surgem externamente dos ambientes técnicos, sociotécnicos, históricos, legais, econômicos ou políticos nos quais ocorrem o projeto, desenvolvimento e implantação de sistemas de IA e que, por isso, são menos controláveis, assim como os fatores de risco

---

[115] CRUZ, Francisco Brito (Coord.); MASSARO, Heloisa; OLIVA, Thiago; BORGES, Ester. *Internet e eleições no Brasil:* diagnósticos e recomendações. 1ª edição, São Paulo: InternetLab, 2019. p. 26. Disponível em: https://www.internetlab.org.br/wp-content/uploads/2019/09/policy-infopol-26919_4.pdf. Acesso em: 05 mai. 2022.
[116] *Ibidem*.

modificáveis, como os levantados internamente das práticas reais de produção e uso de tecnologias de IA, e que, portanto, são mais controláveis.[117]

Ao finalizar o questionário, os fatores apresentados poderão ser classificados em três categorias: a) Fator de risco proibitivo; b) Fator de risco importante e; c) Fator de risco moderado.

Na primeira situação estão incluídos determinantes de danos potenciais que desencadeiam o princípio da precaução e ensejam medidas preventivas para evitar impactos adversos nos direitos humanos e liberdades fundamentais das pessoas afetadas, na democracia e no Estado de Direito. Medidas preventivas são apropriadas quando a gravidade e a escala sobre a possibilidade de remediação do dano potencial superam os níveis de redução e mitigação de riscos.

Quanto à segunda, indicam a presença de determinantes de danos potenciais que estão diretamente ou indiretamente associados a riscos significativos de impactos adversos nos direitos humanos e liberdades fundamentais das pessoas afetadas, na democracia e no Estado de Direito, mas que oferecem oportunidades de redução e mitigação de riscos que tornam os riscos apresentados toleráveis.

Já em relação ao risco moderado, indicam a presença de determinantes de danos potenciais que estão diretamente ou indiretamente associados a riscos de impactos adversos nos direitos humanos e liberdades fundamentais das pessoas afetadas, na democracia e no Estado de Direito, mas que oferecem oportunidades de redução e mitigação de riscos que tornam os riscos apresentados amplamente aceitáveis.[118]

As classificações são indicadas em um relatório resumo gerado ao final das respostas, além disso, este oferece sugestões para cada uma dessas respostas, que direcionam para ações específicas a serem tomadas no processo de avaliação de impacto e para metas, propriedades e áreas específicas nas quais é necessário concentrar os processos subsequentes de gestão de risco e garantia, a fim de reduzir e mitigar os riscos associados.

Este exemplo demonstra que a utilização de inteligência artificial combinada com processamento de dados não requer que direitos humanos e o exercício da cidadania sejam implicados no percurso. Conforme mencionados no capítulo anterior, a tecnologia possui alto

---

[117] LESLIE, David; BURR, Christopher; AITKEN, Mhairi. KATELL, Michael. BRIGGS, Morgan. RINCON, Cami. *Human Rights, Democracy, and the Rule of Law Assurance Framework for AI Systems:* A Proposal. Setembro de 2021. Disponível em: http://dx.doi.org/10.2139/ssrn.4027875. Acesso em: 10 jun. 2023. p. 62.
[118] *Ibidem*, p. 64.

poder transformador, pode e deve ser aliada dos seres humanos, bastando que adaptações como esta sejam cada vez mais utilizadas.

Abordaremos agora a utilização de sistemas de coleta de dados em conjunto com a inteligência artificial pela administração pública, uma vez que o mencionado fator transformador não deve ficar restrito à esfera privada, pois pode aprimorar também a prestação do serviço público. Ainda que, neste caso, os cuidados devam ser ainda maiores e a falta de governança possa acarretar riscos mais significativos.

A Transparência Brasil, em conjunto com diversas organizações da sociedade civil,[119] elaborou em 2020 um documento com recomendações. Este foi produzido após um levantamento dos envolvidos que apontou o uso de quarenta e quatro ferramentas de IA por órgãos governamentais, sendo estas divididas em duas dimensões. A primeira avalia se a aplicação utiliza a tecnologia para tomada de decisões e a segunda considera se o público-alvo é interno ou externo ao poder público.[120]

Um exemplo da primeira dimensão é a ferramenta Bem-te-vi, utilizada pelo Tribunal Superior do Trabalho para classificação de processos e previsões sobre a tramitação do processo nos gabinetes. Nesta situação, caso a aplicação seja ampliada e passe a utilizar decisões automatizadas para motivar decisões judiciais, teremos em questão os direitos relacionados ao devido processo legal e a necessidade de decisões fundamentadas.

Ainda na dimensão em questão, podemos mencionar a plataforma Victor, utilizada pelo Supremo Tribunal Federal, como exemplo de aplicação em que não há a possibilidade de tomada de decisões. Uma vez que o objetivo é simplificar o reconhecimento de padrões em textos jurídicos apresentados. Esta possui capacidade para analisar os recursos extraordinários e identificar quais estão vinculados a determinados temas de repercussão geral.[121]

Quanto à segunda categoria, conforme mencionado acima, há a divisão utilizando como critério o público-alvo. Isto é interno, ao tratar dos próprios agentes governamentais que interagem com a ferramenta; e externo, ao considerar cidadãos, empresas e demais entidades que são impactadas pelo uso da ferramenta.

---

[119] Também participaram da elaboração: Artigo 19; Conectas Direitos Humanos; Instituto Brasileiro de Defesa do Consumidor (IDEC); Instituto de Defesa do Direito de Defesa (IDDD); Instituto de Estudos da Religião (ISER); Instituto de Referência em Internet e Sociedade (IRIS); Instituto de Tecnologia e Sociedade (ITS); Instituto Igarapé; Instituto Socioambiental (ISA); Minas Programam; Mulheres Negras Decidem e; PretaLab.

[120] BURG, Tamara; GALDINO, Manoel; SAKAI, Juliana. *Recomendações de governança:* Uso de inteligência artificial pelo poder público. Transparência Brasil. Fevereiro de 2020. p. 6. Disponível em: https://www.transparencia.org.br/downloads/publicacoes/Recomendacoes_Governanca_Uso_IA_PoderPublico.pdf. Acesso em: 10 jun. 2023.

[121] *Ibidem*, p. 8.

Da análise em questão é possível extrair que a maioria consiste em aplicações com poder de decisão e utilizadas internamente, sendo estas, vinte das quarenta e quatro. O segundo lugar fica com as sem tomada de decisão, mas também utilizadas pelo público interno, sendo dezesseis. Ainda, oito aplicações contam com a funcionalidade da decisão, mas são direcionadas ao público externo. A avaliação acima é necessária para que as recomendações não sejam genéricas, mas sim demonstrem aderência com a realidade.

Para as organizações, o principal fator de risco está relacionado à base de dados de aprendizado e aos parâmetros a serem empregados pelos modelos automatizados de previsão e classificação, utilizados pelas instituições governamentais, os quais podem resultar na reprodução de uma discriminação social já existente, afetando principalmente uma parcela da população que se encontra em situação de maior vulnerabilidade social.

Outra preocupação diz respeito à utilização dos chamados "chatbots", elaborados com o propósito de orientar o utilizador de um serviço público e facilitar o acesso. Neste caso, a preocupação não é com a tecnologia ou proteção de dados, mas sim com a acessibilidade, uma vez que a inclusão digital de grupos como analfabetos, imigrantes e/ou pessoas com deficiência precisa ser considerada.[122]

Considerando não apenas as destacadas acima, mas diversos outros motivos de cuidado mencionados no texto, foram estruturadas quatro recomendações de governança. São elas: 1) Bases de dados representativas e apropriadas para o contexto; 2) Necessidade de supervisão humana como salvaguarda para a revisão de decisões automatizadas; 3) Efetiva proteção dos dados pessoais do cidadão e; 4) Transparência e explicabilidade dos sistemas.

Em relação à primeira, o objetivo é evitar e reduzir/atenuar os vieses dos algoritmos e dos conjuntos de dados de aprendizado que poderiam fortalecer cenários de opressão estrutural (como racismo, machismo, LGBTQIA+fobia, entre outros) em serviços governamentais e investigações do sistema de segurança. Neste caso, há ainda a recomendação de que as bases de dados utilizadas incluam representações das populações presumivelmente afetadas, além da produção de relatórios de impacto.[123]

---

[122] BURG, Tamara; GALDINO, Manoel; SAKAI, Juliana. *Recomendações de governança:* Uso de inteligência artificial pelo poder público. Transparência Brasil. Fevereiro de 2020. p. 11-13. Disponível em: https://www.transparencia.org.br/downloads/publicacoes/Recomendacoes_Governanca_Uso_IA_PoderPublico.pdf. Acesso em: 10 jun. 2023.

[123] *Ibidem*, p. 19-20.

Quanto à segunda recomendação, necessário mencionar que a LGPD, em seu artigo 20[124], concede ao titular o direito de solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses. Entretanto, a lei impõe a condicionante de que a decisão deve ser tomada unicamente com base em tratamento automatizado para obter o direito de revisão, o que pode configurar um desafio para a efetivação do direito, uma vez que o resultado alcançado por meio de ferramentas de decisões automatizadas é empregado para influenciar a tomada de decisão governamental. Contudo, não é possível afirmar que uma determinada ação tenha sido executada unicamente de maneira automatizada pela inteligência artificial.[125]

No que diz respeito à efetiva proteção dos dados pessoais do cidadão, as recomendações são no sentido de observar as instruções da LGPD expressas nos artigos 6, inciso X[126] e 23, inciso I,[127] de forma que a obtenção dos dados deve ser realizada de forma restrita para fornecer e aprimorar o serviço proposto, com uma finalidade adequada, claramente estabelecida e com critérios sujeitos à conformidade dos direitos fundamentais, sendo imprescindível que as pessoas sejam devidamente esclarecidas sobre a finalidade da obtenção de seus dados pessoais e a maneira como estão sendo empregados, de forma transparente.[128]

Por fim, aqui o objetivo da transparência e explicabilidade dos sistemas está atrelado às noções de "*accountability*", isto é, a necessidade de assegurar o acesso a dados públicos referentes aos algoritmos utilizados pelo setor governamental. Para além das questões

---

[124] Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

[125] BURG, Tamara; GALDINO, Manoel; SAKAI, Juliana. *Recomendações de governança:* Uso de inteligência artificial pelo poder público. Transparência Brasil. Fevereiro de 2020. p. 21-22. Disponível em: https://www.transparencia.org.br/downloads/publicacoes/Recomendacoes_Governanca_Uso_IA_PoderPublico.pdf. Acesso em: 10 jun. 2023.

[126] Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
X - Responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

[127] Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:
I - Sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos.

[128] BURG, Tamara; GALDINO, Manoel; SAKAI, Juliana. *Recomendações de governança:* Uso de inteligência artificial pelo poder público. Transparência Brasil. Fevereiro de 2020. p. 23-24. Disponível em: https://www.transparencia.org.br/downloads/publicacoes/Recomendacoes_Governanca_Uso_IA_PoderPublico.pdf. Acesso em: 10 jun. 2023.

mencionadas anteriormente, esta recomendação possui fundamento até mesmo na exigência de avaliar a eficiência de tais ferramentas.

Nesse sentido as sugestões encontradas pelos autores contemplam a adoção de algoritmos de IA com códigos abertos. Estes devem ser acompanhados por explicações de operação do algoritmo, do conjunto de dados utilizado para aprendizado e, se viável, o próprio conjunto de dados utilizado ou uma versão com identidade oculta.

Ademais, também é indicado a implementação de mecanismos de transparência ativa em que seja possível para o cidadão obter a listagem de quais sistemas algorítmicos estão sendo empregados pelo setor governamental, em que contextos e de que maneira, assim como a realização periódica de auditorias do funcionamento do algoritmo, por especialistas externos à empresa ou órgão público.

Além disso, assegurar a transparência dos algoritmos, ou seja, possibilitar ao cidadão compreender o modo de operação do algoritmo, como uma decisão específica foi tomada, sua finalidade e embasamento, além dos dados utilizados no processamento e elaboração e publicização de Relatório de Impacto Algorítmico prévio à operação.[129]

Nesse sentido, Araújo, Zullo e Torres destacam a necessidade da elaboração de métricas que possam assegurar a qualidade dos dados, além de um acompanhamento ativo sobre as funcionalidades existentes e seus riscos pela Autoridade Nacional de Proteção de Dados (ANPD) – criada pela Lei número 13.853 de 2019.[130]

Assim, desde o final dos anos 90 que Lawrence Lessig defende a prioridade de elaborar regulações com foco na integridade de princípios legais fundamentais, como liberdade de expressão, privacidade e propriedade intelectual. Sem deixar de lado, evidentemente, as peculiaridades tecnológicas e as formas emergentes de interação e comunicação.[131]

Para o autor, há que se considerar os aspectos técnicos do ciberespaço ao formular políticas e leis, e destaca a necessidade de flexibilidade para que as regulamentações possam se

---

[129] BURG, Tamara; GALDINO, Manoel; SAKAI, Juliana. *Recomendações de governança:* Uso de inteligência artificial pelo poder público. Transparência Brasil. Fevereiro de 2020. p. 25-26. Disponível em: https://www.transparencia.org.br/downloads/publicacoes/Recomendacoes_Governanca_Uso_IA_PoderPublico.pdf. Acesso em: 10 jun. 2023.

[130] ARAÚJO, Valter Shuenquener de; ZULLO, Bruno Almeida; TORRES, Maurílio. Big data, algoritmos e inteligência artificial na administração pública: reflexões para a sua utilização em um ambiente democrático. *A&C - Revista de Direito Administrativo & Constitucional*, volume 20, nº 80. p. 258, setembro de 2020. Revista de Direito Administrativo and Constitucional. Disponível em: http://dx.doi.org/10.21056/aec.v20i80.1219. Acesso em: 10 jun. 2023.

[131] LESSIG, Lawrence. The Law of the Horse: what cyberlaw might teach. *Harvard Law Review*, volume 113, nº 2, p. 543-545, dezembro de 1999. Disponível em: http://dx.doi.org/10.2307/1342331. Acesso em: 13 mai. 2023.

adaptar às rápidas mudanças tecnológicas.[132] Tal entendimento pode ser estendido às aplicações de inteligência artificial que utilizam o processamento de dados.

As recomendações acima estão em conformidade com as elaboradas por organizações internacionais e nacionais já mencionadas. Dessa forma, imprescindível lembrar que, ao debater e apresentar sugestões de governança para a utilização de algoritmos de IA, é fundamental levar em conta a análise de perigos reais e possíveis para direitos e para o espaço cívico, visando conciliar impulsionar inovação e tecnologia com responsabilidade social e transparência.

2.2 FORMAS DE TRATAMENTO DE DADOS E REVISÃO DE DECISÕES AUTOMATIZADAS

Depois de analisar a jornada da proteção de dados como direito autônomo até o seu reconhecimento como aspecto da personalidade e, portanto, direito fundamental, permeando as implicações deste na vida das pessoas, inclusive na esfera pública, nota-se que a capacidade computacional anteriormente explorada, associada ao processamento de quantidades massivas de dados, pode resultar em inferências relacionadas à tomada de decisão. Passaremos a explorar as formas de tratamento destes dados e o funcionamento de decisões automatizadas.

Para Juliana Abrusio, por decisão automatizada podemos compreender:[133]

> Aquela assim considerada quando realizada com base em dados pessoais processados artificialmente por meio de algoritmos, tendo como resultado a elaboração de conjuntos de informações estruturadas ou "definição de perfis", capazes de permitir análises e predições (por humanos ou mesmo por máquinas) de comportamentos e até atitudes morais do interessado.

A autora alerta também que um dos principais riscos das escolhas feitas por meio de processamento automatizado é a falsa sensação e semblante de que, precisamente por não contar com intervenção humana na tomada de decisão, esta seria mais imparcial, o que não é necessariamente verídico.[134] Tal suposição também ocorre com diversas aplicações que utilizam inteligência artificial.

A União Europeia publicou no ano de 1995 a Diretiva 95/46/CE, que dispõe sobre proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. A preocupação quanto às decisões automatizadas está presente em

---

[132] LESSIG, Lawrence. The Law of the Horse: what cyberlaw might teach. *Harvard Law Review*, volume 113, nº 2, p. 522, dezembro de 1999. Disponível em: http://dx.doi.org/10.2307/1342331. Acesso em: 13 mai. 2023.
[133] ABRUSIO, Juliana. *Proteção de dados na cultura do algoritmo*. Belo Horizonte: D'Plácido, 2020. p. 254-255.
[134] *Ibidem*, p. 255.

diversos momentos ao longo do diploma legal, entretanto, no artigo 15 podemos observar diretamente a vedação a este tipo de prática.[135]

A Diretiva mencionada surgiu em decorrência da necessidade de assegurar aos cidadãos europeus a denominada "autodeterminação informacional", ou seja, o completo domínio sobre suas informações pessoais, ainda que tenha proporcionado alguma elasticidade aos países membros do bloco ao adaptar as normas às suas leis internas.

Esta foi superada quanto ao critério de aplicação ao ser editado no ano de 2016 o já mencionado Regulamento Geral sobre a Proteção de Dados, que estabelece, dentre outras preocupações, que todos os tratamentos envolvendo dados pessoais de cidadãos europeus, pouco importando se os responsáveis por esses tratamentos são pessoas físicas ou jurídicas, não europeus e com sede fora da União Europeia.[136]

Ainda, o Regulamento aumenta consideravelmente a variedade de operações que agora são classificadas como tratamento de informações pessoais, e ampliou a definição de dados pessoais, abrangendo informações que permitem identificar ou tornar identificável um indivíduo, abarcando dados genéticos, biométricos, fisiológicos, comportamentais, como imagens faciais e informações datiloscópicas.[137]

As decisões automatizadas, por sua vez, possuem uma esfera de aplicação distinta e podem ser executadas em conjunto com a prática de criação de perfis. Isso ocorre porque a "criação de perfis" acontece por meio de processamento automatizado, embora não necessariamente envolva decisões automatizadas. Por outro lado, em um processo iniciado com uma decisão automatizada, posteriormente, pode-se realizar um procedimento fundamentado em criação de perfis.[138]

Exemplificando o raciocínio anterior, a decisão pode ser puramente humana, porém embasada em criação de perfis quando, por exemplo, um indivíduo decide se um crédito deve ser ou não concedido, com base em um perfil elaborado de maneira automatizada, com a

---

[135] Artigo 15º - Decisões individuais automatizadas - 1. Os Estados-membros reconhecerão a qualquer pessoa o direito de não ficar sujeita a uma decisão que produza efeitos na sua esfera jurídica ou que a afecte de modo significativo, tomada exclusivamente com base num tratamento automatizado de dados destinado a avaliar determinados aspectos da sua personalidade, como por exemplo a sua capacidade profissional, o seu crédito, confiança de que é merecedora, comportamento.

[136] COLOMBO, Cristiano; FACCHINI NETO, Eugênio. Mineração de dados e análise preditiva: reflexões sobre possíveis violações ao direito de privacidade na sociedade da informação e critérios para sua adequada implementação à luz do ordenamento brasileiro. *Revista de Direito, Governança e Novas Tecnologias*, Florianópolis, v. 3, n. 2, p. 59, 2 dez. 2017. Conselho Nacional de Pesquisa e Pós-Graduação em Direito - CONPEDI. Disponível em: http://dx.doi.org/10.26668/indexlawjournals/2526-0049/2017.v3i2.2345. Acesso em: 13 set. 2023.

[137] *Ibidem*.

[138] ABRUSIO, Juliana. *Proteção de dados na cultura do algoritmo.* Belo Horizonte: D'Plácido, 2020. p. 259.

finalidade específica de análise. Essa mesma decisão poderia ser tomada sem intervenção humana, ou seja, de maneira totalmente automatizada, por meio de um algoritmo decidindo e informando à pessoa sobre o desfecho da concessão do empréstimo.

Conforme mencionado anteriormente, os dados são uma expressão da personalidade de uma pessoa, sendo assim, a qualidade e atualização das informações produzidas com base neles são aprimoradas, e no funcionamento ideal de um sistema, sua identidade é mais bem representada ao exercer um controle eficaz sobre os dados.

A probabilidade de que os direitos individuais de gestão de informações, estabelecidos com base na preservação da privacidade, possam atuar como um relevante mecanismo, não apenas diante de dados interpretados por seres humanos, mas também perante o processamento de conjuntos de dados por meio de tecnologias de *big data* e algoritmos de perfilagem.[139]

A LGPD define tratamento no Art. 5º, inciso X.[140] A referida lei também elenca em seu Art. 3º[141] os requisitos para sua aplicabilidade e exclui de sua abrangência os tratamentos de dados realizados por pessoa natural para fins exclusivamente particulares e não econômicos. Uma das técnicas mais reconhecidas de tratamento de dados é a chamada "*profiling*", que consiste na elaboração de perfis de comportamento de uma pessoa a partir de informações que ela disponibiliza ou que são colhidas.[142] A referida técnica pode ser utilizada tendo como objetivo indivíduos ou grupos.

As informações são processadas por meio de abordagens estatísticas e técnicas de IA, visando adquirir uma "metainformação", que envolveria uma compilação dos padrões, gostos pessoais e demais registros da existência dessa pessoa.[143] Em outras palavras, as aplicações são

---

[139] MARTINS, Pedro; HOSNI, David. O Livre Desenvolvimento da Identidade Pessoal em Meio Digital: Para além da proteção da privacidade? *In:* PASQUOT, Fabrício Bertini; ANJOS, Lucas Costa dos; BRANDÃO, Luíza Couto Chaves. (Org.). *Políticas, Internet e Sociedade.* 1ed. Belo Horizonte: IRIS, 2019, v., p. 46-5. Disponível em: http://dx.doi.org/10.2139/ssrn.3464025. Acesso em: 12 set. 2023.

[140] Art. 5º Para os fins desta Lei, considera-se:
X- Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

[141] Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:
I - a operação de tratamento seja realizada no território nacional;
II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou
III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

[142] DONEDA, Danilo. *Da Privacidade à Proteção de Dados Pessoais:* Fundamentos da Lei Geral de Proteção de Dados. 3ª edição, São Paulo: Thomson Reuters Brasil, 2021. p. 155.

[143] *Ibidem*, p. 156.

estruturadas para encontrar padrões e probabilidades, e resultam na criação de perfis de indivíduos, grupos, lugares, eventos ou qualquer coisa de interesse.

O produto pode ser empregado para delinear um panorama das inclinações de futuras escolhas, condutas e destino de um indivíduo ou conjunto. O uso de métodos atuariais nesse contexto tem a finalidade de gerar informações prognósticas para antecipar tendências futuras e prever comportamentos, processos ou desenvolvimentos. O objetivo é desenvolver estratégias para gerenciar as incertezas do futuro no presente.[144]

Para Abrusio, a forma em questão se desenvolve ao redor de três elementos básicos: 1) a necessidade do tratamento automatizado (exclusivo ou híbrido combinado com intervenção humana); 2) deve ser implementada em relação a dados pessoais e; 3) com o objetivo de avaliar aspectos pessoais de uma pessoa natural.[145] A autora atenta para o fato de que uma mera categorização de indivíduos com base em atributos fundamentais, como idade, gênero, peso e estatura, não implica, obrigatoriamente, na aplicação de perfilamento.

A metodologia pode possuir diversas utilidades, desde o monitoramento da admissão de indivíduos em uma nação específica pelos órgãos alfandegários, até o uso com fins particulares, como o envio de mensagens promocionais. Um perfil adquirido dessa forma pode se converter em uma autêntica representação virtual do indivíduo, constituindo o único aspecto visível desta pessoa para outros com quem interaja.[146]

Também são exemplos de decisões tomadas de maneira automatizada, a relacionada a concessão ou não de um financiamento (considerando a postura da pessoa em relação ao adimplemento de pagamentos), a não atribuição de determinado trabalho (tomando como base sua atitude relacional em grupos de trabalho) a uma pessoa ou a sujeição de um indivíduo a um processo de matéria fiscal (analisando seu volume de negócios).[147]

A partir do momento em que um perfil digital se torna a única faceta visível da personalidade de alguém para os outros, as técnicas de previsão de padrões de conduta podem resultar em uma restrição de sua esfera de autonomia, uma vez que diversos indivíduos com quem interage presumem que ela adote um comportamento predefinido.

Isso pode acarretar uma possível diminuição de sua liberdade de escolha, já que muitas de suas potencialidades e oportunidades podem ser previamente moldadas com base nessas

---

[144] BOSCO, Francesca et al. Profiling technologies and fundamental rights and values: regulatory challenges and perspectives from European Data Protection Authorities. *Reforming European data protection law*, 2014, p. 3-33, 2015. Disponível em: https://link.springer.com/chapter/10.1007/978-94-017-9385-8_1. Acesso em: 18 set. 2023.
[145] ABRUSIO, Juliana. *Proteção de dados na cultura do algoritmo*. Belo Horizonte: D'Plácido, 2020. p. 258.
[146] DONEDA, Danilo. *Da Privacidade à Proteção de Dados Pessoais:* Fundamentos da Lei Geral de Proteção de Dados. 3ª edição, São Paulo: Thomson Reuters Brasil, 2021. p. 156.
[147] ABRUSIO, Juliana. *Proteção de dados na cultura do algoritmo*. Belo Horizonte: D'Plácido, 2020. p. 255.

suposições.[148] Nesse sentido, relevante mencionar que o perfil criado não tem como propósito único criar padrões descritivos sobre alguém, mas também pode ser utilizado para verificar outros padrões inicialmente gerados.

Adicionam-se às preocupações mencionadas outras particularidades distintivas da perfilagem resultantes do procedimento automatizado, realizado através de algoritmos: a ausência de determinação de causas ou motivos para o surgimento ou a manutenção das relações identificadas; a correspondência da precisão do procedimento com a quantidade de dados coletados, tornando o princípio da minimização de dados problemático; e a disparidade informacional criada entre o titular e o controlador de dados.[149] A partir disto, é possível concluir que a assimetria de poder entre o titular e as empresas ou entidades governamentais detentoras de tecnologias de processamento de dados em massa é acentuada pela escassez de informações.

Em relação ao parágrafo anterior também é possível infirmar que a avaliação de *Big Data* é, em essência, tanto mais eficaz quanto maior for a disponibilidade de dados diversos e de diferentes procedências, que podem ser examinados de variadas maneiras e cujas conclusões podem ser aplicadas em diversos cenários.[150] Isso também vai de encontro ao princípio da minimização - este será abordado com mais profundidade posteriormente.

O perfilamento é visto como uma tecnologia cativante: ele sugere que as pessoas podem adquirir conhecimentos imprevisíveis que possibilitam tomar decisões mais acertadas. Contudo, o aspecto negativo do perfilamento reside no fato de que ele "[...] oculta tudo o que não pode ser convertido em informações legíveis por máquinas",[151] tais como decisões médicas que consideram a subjetividade de cada ser. Ainda, retornando a discussão para o ponto central, se faz necessário lembrar a importância dos direitos relacionados à transparência e explicação de decisões envolvendo métodos automatizados.

Nesse sentido, outro fator que representa uma ameaça ao crescimento independente da identidade é a capacidade de deduzir conclusões a partir de dados adquiridos através das ações do titular. Mediante a análise de um conjunto de informações disponibilizado de forma legal,

---

[148] DONEDA, Danilo. *Da Privacidade à Proteção de Dados Pessoais:* Fundamentos da Lei Geral de Proteção de Dados. 3ª edição, São Paulo: Thomson Reuters Brasil, 2021. p. 156.

[149] MARTINS, Pedro. HOSNI, David, O Livre Desenvolvimento da Identidade Pessoal em Meio Digital: Para além da proteção da privacidade? *In:* PASQUOT, Fabrício Bertini; ANJOS, Lucas Costa dos; BRANDÃO, Luíza Couto Chaves. (Org.). *Políticas, Internet e Sociedade.* 1ed. Belo Horizonte: IRIS, 2019, v., p. 46-5. Disponível em: http://dx.doi.org/10.2139/ssrn.3464025. Acesso em: 12 set. 2023.

[150] WOLFGANG, Hoffmann-Riem. *Teoria Geral do Direito Digital*. São Paulo: Grupo GEN, 2021. p. 114. Disponível em: https://app.minhabiblioteca.com.br/#/books/9786559642267/. Acesso em: 28 set. 2023.

[151] BOSCO, Francesca *et al*. Profiling technologies and fundamental rights and values: regulatory challenges and perspectives from European Data Protection Authorities. *Reforming European data protection law*, 2014, p. 3-33, 2015. Disponível em: https://link.springer.com/chapter/10.1007/978-94-017-9385-8_1. Acesso em: 18 set. 2023.

torna-se viável deduzir detalhes que o titular nunca teve a intenção de divulgar. Assim, informações confidenciais são deduzidas a partir de dados que, inicialmente, não seriam classificados como informações pessoais sensíveis.[152]

Na tecnologia mencionada, tudo é ajustado com base nesses padrões pré-concebidos, inclusive o próprio conteúdo explorado na internet, desde a interação do usuário com outras pessoas em uma plataforma de mídia social, até o acesso e a pesquisa por informações. A pessoa se torna o próprio conteúdo, uma informação que orbita em torno de interesses deduzidos por meio de seus dados.[153]

A combinação dessas diferentes variáveis destaca que a proteção das informações individuais envolve diretamente o curso da existência das pessoas, atravessando de forma abrangente seus diversos vínculos sociais, desde o estabelecimento de acordos e a prática de consumo, até mesmo a busca pelo acesso à informação. No âmbito do "*big data*", são os algoritmos que assumem a função de coordenar a existência das pessoas, determinando suas possibilidades.[154]

A proteção de dados ainda está associada à defesa da privacidade, é importante considerar não apenas o seu aspecto negativo, mas também a oportunidade para o titular comunicar dados de forma relevante para o controlador, permitindo, portanto, a afirmação de uma história pessoal e, como resultado, uma influência na forma como será avaliado com base no seu perfil. Configurando, assim, o direito de controle sobre como se é percebido.[155]

Em artigo recente, pesquisadores dos cursos de tecnologia da Pontifícia Universidade Católica elencaram os principais desafios para as aplicações envolvendo perfilamento. A publicação foi elaborada por meio de revisão de literatura sobre como o perfil de dados está sendo usado nos ecossistemas de *big data*.

Dos treze catalogados, mencionaremos os cinco primeiros, considerando que foram ordenados pelo critério do número de ocorrências nas demais publicações. São eles: a) Complexidade – o perfilamento é uma operação complexa que faz parte do processo de preparação de dados, sendo assim, a variedade e o volume criam desafios para a capacidade

---

[152] MARTINS, Pedro. HOSNI, David. O Livre Desenvolvimento da Identidade Pessoal em Meio Digital: Para além da proteção da privacidade? *In:* Fabrício Bertini Pasquot; Lucas Costa dos Anjos; Luíza Couto Chaves Brandão. (Org.). *Políticas, Internet e Sociedade.* 1ed. Belo Horizonte: IRIS, 2019, v., p. 46-5. Disponível em: http://dx.doi.org/10.2139/ssrn.3464025. Acesso em: 12 set. 2023.

[153] BIONI, Bruno R. *Proteção de Dados Pessoais:* A Função e os Limites do Consentimento. 3ª edição. Rio de Janeiro: Forense, 2021, p. 88-89.

[154] *Ibidem*, Pp 89.

[155] MARTINS, Pedro. HOSNI, David. O Livre Desenvolvimento da Identidade Pessoal em Meio Digital: Para além da proteção da privacidade? *In:* Fabrício Bertini Pasquot; Lucas Costa dos Anjos; Luíza Couto Chaves Brandão. (Org.). *Políticas, Internet e Sociedade.* 1ed. Belo Horizonte: IRIS, 2019, v., p. 46-5. Disponível em: http://dx.doi.org/10.2139/ssrn.3464025. Acesso em: 12 set. 2023.

computacional, como, por exemplo, requisitos de memória; b) Perfil contínuo - atualizar automaticamente o perfil de dados em tempo real é desafiador porque requer que os algoritmos de perfil de dados estejam sempre em execução e consome recursos que poderiam ser usados para outras tarefas; c) Perfil incremental - atualização do perfil de dados de acordo com um determinado intervalo de tempo; d) Interpretação - ser capaz de compreender e interpretar os resultados do perfil de dados; e e) Falta de pesquisa - os autores afirmam que não há muita pesquisa sobre o tema.[156]

As dificuldades apresentadas dizem respeito a parte técnica das ferramentas que utilizam a tecnologia em questão e não às questões jurídicas. Entretanto, ao adicionar a inteligência artificial à reflexão é inevitável não se deparar com tais dificuldades de igual forma. Além disso, necessário sopesar o impacto dela em tais obstáculos, concluindo que existe uma chance considerável de reduzi-los severamente, dada sua maior capacidade de processamento. O que também pode indicar uma retomada em pesquisas sobre o assunto.

A criação de perfis e as escolhas individuais automatizadas, independentemente de envolverem ou não a elaboração de perfis, devem ser regidos pelos princípios da proteção de dados, possuir fundamentos adequados para o processamento das informações pessoais e sempre garantir o direito de oposição e explicação. Assim, o responsável pelo processamento deve fornecer ao titular dos dados informações sucintas, transparentes, compreensíveis e de fácil acesso sobre o tratamento de suas informações pessoais, com uma finalidade específica.

Outra técnica com reconhecimento significativo é o chamado "*data mining*" que pode ser compreendido como a extração não trivial de informações implícitas, anteriormente desconhecidas e potencialmente úteis a partir de dados.[157] Uma característica de extrema relevância na definição da mineração de dados é a de que não se limita à coleta de dados organizados ou não, como um objetivo final. Na realidade, é um procedimento com fases a serem seguidas, com um propósito particular.[158]

---

[156] COUTO, Júlia Colleoni *et al*. New trends in big data profiling. *In: Science and Information Conference.* Cham: Springer International Publishing, 2022. p. 808-825. Disponível em: http://dx.doi.org/10.1007/978-3-031-10461-9_55. Acesso em: 14 set. 2023.

[157] "Data mining [...] is the nontrivial extraction of implicit, previously unknown, and potentially useful information from data". SCHERMER, Bart W. The limits of privacy in automated profiling and data mining. *Computer Law & Security Review*, volume 27, nº 1, p. 45-52, 2011. Disponível em: https://doi.org/10.1016/j.clsr.2010.11.009. Acesso em: 12 jun. 2023.

[158] COLOMBO, Cristiano; FACCHINI NETO, Eugênio. Mineração de dados e análise preditiva: reflexões sobre possíveis violações ao direito de privacidade na sociedade da informação e critérios para sua adequada implementação à luz do ordenamento brasileiro. *Revista de Direito, Governança e Novas Tecnologias*, Florianópolis, v. 3, n. 2, p. 59, 2 dez. 2017. Conselho Nacional de Pesquisa e Pós-Graduação em Direito - CONPEDI. Disponível em: http://dx.doi.org/10.26668/indexlawjournals/2526-0049/2017.v3i2.2345. Acesso em: 13 set. 2023.

A questão da mineração está intimamente ligada à preservação de informações, a qual, considerando a legislação em vigor em cada país e a presença ou ausência de uma entidade oficial competente para a proteção de dados, pode atribuir menos ou mais importância ao direito à privacidade do indivíduo.

Uma definição mais técnica seria, em termos simplificados, a extração de dados pode ser caracterizada como um procedimento automatizado ou semiautomatizado para investigar analiticamente grandes conjuntos de dados, com o intuito de identificar padrões significativos presentes nos dados, os quais desempenham um papel crucial na aquisição de informações relevantes e no apoio à criação de conhecimento.[159]

A ferramenta pode ser considerada de importância fundamental dentro do contexto atual e sua capacidade de organizar informações a partir de uma quantidade elevada de dados em estado bruto. Ao analisar uma vasta quantidade de dados não processados e não categorizados, torna-se viável identificar informações de potencial interesse. Tal possibilidade aumenta à medida que a quantidade de informações não processadas disponíveis também aumenta, bem como o avanço das técnicas para extrair a informação considerada valiosa.

A coleta e retenção de informações é inestimável e à vista humana, inacessível, no entanto, não é o ser humano que está no comando e conduz a avaliação dessas enormes quantidades de dados. A mineração de dados explora a otimização do uso de vastos bancos de dados que seriam limitados em uma situação analógica. Além disso, a avaliação de amplos e heterogêneos conjuntos de dados - o que possibilita atualmente precisas análises prognósticas e a revelação de inúmeras associações previamente não identificadas - ultrapassa a habilidade do ser humano.

Essa dinâmica traz consigo consequências relacionadas às informações pessoais. A quantidade de dados disponíveis sobre um indivíduo em diferentes bancos de dados aumenta, e essas informações têm o potencial de impactar sua vida futura. Uma simples pesquisa na Internet pelo nosso nome ou pelo nome de pessoas conhecidas pode, em muitos casos, revelar o impacto concreto do registro não intencional de informações sobre nós.[160]

Imprescindível ressaltar que o principal desafio na abordagem das técnicas mencionadas - assim como em muitas outras - reside no perigo de cair em uma simplificação excessiva que negligencia outras aplicações da tecnologia - e até mesmo da concepção de uma

---

[159] SILVA, Leandro Augusto da; PERES, Sarajane M.; BOSCARIOLI, Clodis. *Introdução à Mineração de Dados - Com Aplicações em R.* São Paulo: Grupo GEN, 2016. p. 7. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788595155473/. Acesso em: 23 set. 2023.

[160] DONEDA, Danilo. *Da Privacidade à Proteção de Dados Pessoais:* Fundamentos da Lei Geral de Proteção de Dados. 3ª edição, São Paulo: Thomson Reuters Brasil, 2021. p. 159.

"*persona virtual*" - que podem ser benéficas e até mesmo essenciais para o desenvolvimento da identidade pessoal ou para outros propósitos que não necessariamente confrontam interesses protegidos.[161]

Nesse sentido, as informações individuais não podem ser encaradas como itens de uma "fonte inesgotável", na qual atores do universo digital possam se utilizar sem restrições, fornecendo insumos a algoritmos computacionais com o único propósito de obter ganhos financeiros.[162] Além disso, como mencionado previamente, há o risco significativo de informações cruzadas revelarem dados sensíveis que o titular não intentava compartilhar inicialmente.

Sobre isto, Danilo Doneda postula que, neste instante, em vez de uma investigação minuciosa dessas e de outras abordagens, é importante destacar um componente vital de várias formas de coleta e processamento de informações individuais: a possibilidade de gerar um afastamento entre os dados que uma pessoa fornece conscientemente e o propósito para o qual são transformados.[163]

O autor[164] prossegue ao completar seu raciocínio:

> Os dados pessoais passam em diversas ocasiões a serem intermediários entre a pessoa e a sociedade, prepostos, no entanto, nem sempre autorizados e capazes – e é justamente isto que pode gerar como efeito a perda de controle da pessoa sobre o que se sabe em relação a si mesma – o que, em última análise, representa uma diminuição na sua própria liberdade.

Ao longo deste ponto dissertamos acerca das implicações do tratamento de dados nos direitos à privacidade e principalmente à proteção de dados, de modo que a principal repercussão se dá justamente no mencionado acima, a imagem/"persona" virtual pode restringir a liberdade real e por consequência limitar a personalidade de uma pessoa.

O direito à transparência é de extrema importância neste contexto, como sublinhado ao longo deste capítulo. Este desempenha um papel crucial ao garantir que os indivíduos tenham conhecimento e controle sobre como seus dados são coletados e utilizados, promovendo assim uma abordagem mais justa e equitativa na era da tecnologia da informação.

---

[161] DONEDA, Danilo. *Da Privacidade à Proteção de Dados Pessoais:* Fundamentos da Lei Geral de Proteção de Dados. 3ª edição, São Paulo: Thomson Reuters Brasil, 2021. p. 160.

[162] COLOMBO, Cristiano; FACCHINI NETO, Eugênio. MINERAÇÃO DE DADOS E ANÁLISE PREDITIVA: reflexões sobre possíveis violações ao direito de privacidade na sociedade da informação e critérios para sua adequada implementação à luz do ordenamento brasileiro. *Revista de Direito, Governança e Novas Tecnologias*, Florianópolis, v. 3, n. 2, p. 59, 2 dez. 2017. Conselho Nacional de Pesquisa e Pós-Graduação em Direito - CONPEDI. Disponível em: http://dx.doi.org/10.26668/indexlawjournals/2526-0049/2017.v3i2.2345. Acessado em: 13 de setembro de 2023.

[163] DONEDA, Danilo. *Da Privacidade à Proteção de Dados Pessoais:* Fundamentos da Lei Geral de Proteção de Dados. 3ª edição, São Paulo: Thomson Reuters Brasil, 2021. p. 161.

[164] *Ibidem*, p. 162.

As operações mencionadas devem fomentar mecanismos que as alinhem com os critérios de proteção da dignidade humana estabelecidos pelos direitos fundamentais, recursos que capacitem as partes envolvidas a exercer um controle eficaz sobre suas informações individuais, assegurando o acesso, a veracidade, a segurança e a compreensão do propósito de sua utilização, entre outros aspectos.

As inquietações neste tópico abordadas, embora mereçam séria consideração, não estão a propor a solução simplória de se proibir a prática da extração de dados, indicando sua proibição. Desde o início da exposição nos posicionamos contrários a tentativas de barrar os avanços tecnológicos e científicos envolvendo dados e/ou inteligência artificial. Além de ser inviável, isso resultaria em uma séria violação do princípio da liberdade econômica.

Conforme abordado anteriormente, o trecho acima alerta para a importância de ponderar acerca do desafio de uma abordagem equilibrada de determinadas técnicas, evitando simplificações excessivas. Essa perspectiva ressalta que tais abordagens têm potencial tanto para beneficiar quanto para serem essenciais no desenvolvimento da identidade pessoal e em outros propósitos. Além disso, destaca-se que essas aplicações não necessariamente entram em conflito com interesses protegidos, evidenciando a importância de balancear as abordagens tecnológicas para considerar uma ampla gama de possibilidades e impactos positivos.

2.3 TRANSPARÊNCIA ALGORÍTMICA

Diversos tipos de publicações, desde artigos científicos à instrumentos legais, apontam a transparência como fator relevante para a estruturação da inteligência artificial levando em conta a proteção de dados. Neste ponto, exploraremos mais sobre suas relações e instrumentalidade.

José Renato Pereira, em artigo intitulado *Transparência pela cooperação*, propõe estratégias regulatórias que podem ser utilizadas para lidar com a opacidade algorítmica, de modo a testar a aplicabilidade da Teoria da Regulação Responsiva, que resumidamente se baseia na cooperação entre regulador e regulado, sistemas de governança em rede e uma pirâmide regulatória para concretizar a proposta do autor.

Nesse sentido, para ele, existem diferentes critérios para classificar o grau de explicabilidade de um sistema de decisões automatizadas, um deles leva em conta o momento

em que o método é aplicável na construção do modelo. Se antes (pré-modelo, *pre-model*), durante (no-modelo, *in-model*) ou depois (pós-modelo, *post-model*) do seu desenvolvimento.[165]

As estratégias de explicação pré-modelo são elaboradas antes da criação efetiva do modelo em si e, consequentemente, são autônomas em relação a ele, aplicando-se exclusivamente aos dados que serão utilizados para alimentar o sistema. Do ponto de vista das normas de proteção de dados, essa abordagem é crucial para avaliar quais dados estão sendo processados pelo sistema. No entanto, sozinha, não possibilita compreender como esses dados estão sendo empregados para chegar a decisões específicas no sistema.

Já as abordagens no-modelo, relacionam-se a protótipos que integram recursos para elucidar suas funcionalidades desde o próprio desenvolvimento, sendo, dessa forma, intrinsecamente interpretáveis. Têm como objetivo responder à indagação de como opera o modelo e, por conseguinte, como realiza o processamento dos dados de treinamento. Por fim, as estratégias pós-modelo, por outro lado, referem-se ao aprimoramento da compreensibilidade de um sistema depois que ele já foi construído.[166]

As estratégias de fomento à compreensibilidade também podem ser classificadas conforme sua abrangência, a qual diz respeito à etapa do processo de predição que buscam elucidar. Elas têm a capacidade de oferecer transparência algorítmica ou interpretabilidade em níveis global e local.

Para Pereira, a transparência algorítmica possibilita compreender como o algoritmo assimila informações dos dados e que tipo de conexões pode derivar dessa operação. Nesse contexto, seu propósito é compreender o funcionamento do algoritmo, e não as previsões individuais. Por sua vez, a interpretabilidade global é aplicada quando o objetivo do agente é descrever o comportamento de todo o modelo, o que inclui uma compreensão dos dados e do próprio algoritmo.[167]

O autor argumenta que diferentes tipos de explicações devem contemplar diferentes grupos interessados, como usuários ou legisladores. Do ponto de vista do usuário, entretanto, é fato que são necessidades heterogêneas e uma mesma pessoa, em situações diferentes, pode buscar mais ou menos explicações, mas nos posicionamos no sentido de que em qualquer uma

---

[165] PEREIRA, José Renato L. de. Transparência pela cooperação: como a regulação responsiva pode auxiliar na promoção de sistemas de *machine-learning* inteligíveis. *Revista de Direito Setorial e Regulatório*, v. 7, nº 1, p. 194-223, maio-junho 2021.
[166] *Ibidem*.
[167] *Ibidem*. O autor compreende interpretabilidade como uma relacão de sistemas intrinsecamente compreensíveis, não demandando explicações adicionais sobre seus mecanismos.

delas (resguardando os direitos de propriedade intelectual e industrial das empresas), estes deveriam ter o acesso concedido e facilitado.

Converter sistemas em termos claros e compreensíveis não se resume apenas a instruir um indivíduo sobre o funcionamento de uma estrutura isoladamente. Também pode ser considerado como uma maneira de resguardar informações pessoais e lidar com a discriminação algorítmica. Assim, o principal objetivo dos regimes de proteção de dados é fornecer aos usuários controle sobre seus dados. Essa é a ideia central que permeia o direito à autodeterminação informacional.[168]

Houve ampla discussão sobre a necessidade de regulamentação dos sistemas de inteligência artificial. Entretanto, dada a complexidade e os perigos associados a esses sistemas, o debate não deve se limitar à dicotomia simplista entre regulamentar e desregulamentar. Deve, em vez disso, concentrar-se em estabelecer parâmetros basilares para elaboração da regulamentação, especialmente no que tange à sua compreensibilidade.

Nesse sentido, para José Renato Pereira, alguns atributos que os órgãos reguladores devem considerar incluem, por exemplo, os períodos de insegurança que um sistema apresenta em relação ao setor no qual será implementado ou à classe de dados pessoais que serão processados. À medida que o risco associado a um sistema aumenta, é provável que também cresça a exigência de transparência, a fim de prevenir eventuais danos que o sistema possa causar.[169]

Dessa forma, como mencionado ao longo deste trabalho, uma regulamentação efetiva deve ser capaz de, por um lado, viabilizar a flexibilidade do órgão regulador para aplicar diversas diretrizes visando distintos sistemas de aprendizado de máquina em contextos variados. Por outro lado, é essencial manter um diálogo contínuo não apenas entre o regulador e os regulamentados, mas também com outras partes envolvidas.

Conforme iniciado neste tópico, o referido autor possui determinados apontamentos para direcionar a regulamentação da inteligência artificial, o principal deles: colaboração essencial entre órgãos reguladores e aqueles sujeitos à regulamentação, uma faceta crucial na qual a teoria se fundamenta para estimular a conformidade por meio de uma negociação eficaz

---

[168] MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a história de um conceito. *Pensar - Revista de Ciências Jurídicas*, v. 25, n. 4, p. 1-18, 11 dez. 2020. Disponível em: http://dx.doi.org/10.5020/2317-2150.2020.10828. Acesso em: 27 set. 2023.

[169] PEREIRA, José Renato L. de. Transparência pela cooperação: como a regulação responsiva pode auxiliar na promoção de sistemas de *machine-learning* inteligíveis. *Revista de Direito Setorial e Regulatório*, v. 7, nº 1, p. 194-223, maio-junho 2021.

entre empresas e entidades governamentais.[170] Tal posicionamento ressoa com o argumentado durante esta exposição.

Os critérios de transparência não estão relacionados apenas à habilidade de discernir a interface de comunicação, mas também ao entendimento dos elementos que são relevantes para compreender o funcionamento do controle baseado em algoritmos. Isso inclui, por exemplo, o planejamento técnico, os parâmetros e ideias da implementação do algoritmo.

A transparência pode ser compreendida também como parte de instrumentos relacionados à uma espécie de prestação de contas ao sujeito de direitos. Dessa forma, há que se atentar também a necessidade de transparência quanto ao tipo de algoritmos e sua utilização, de modo a observar as máximas utilizadas na programação, os critérios utilizados, ou até mesmo que informações são inseridas como *input* e se os algoritmos são utilizados para seleção e controle em casos concretos ("*targeting*", perfil ou em "*scoring*").[171]

Tais questões não serão confrontadas exclusivamente por usuários individuais. As entidades encarregadas de supervisionar a conformidade com a eventual legislação, a autoridade de proteção de dados, também irão se deparar com significativos desafios de informação. Um aspecto central nas análises sobre regulamentação de sistemas de inteligência artificial tem sido a sua falta de transparência, o que levou muitos pesquisadores a caracterizarem tais tecnologias como "caixas pretas".

Isso ocorre principalmente porque diversos sistemas utilizam grandes volumes de dados para identificar padrões que servirão como base para a automação de suas operações, e suas atividades envolvem caminhos complexos para analisar essas informações, como é o caso dos sistemas de aprendizado profundo, como mencionado anteriormente.

Entretanto, a Coalizão Direitos na Rede, em parceria com o Laboratório de Políticas Públicas e Internet, elaborou uma Nota Técnica referente ao Projeto de Lei número 2338/2023, em que apontam que ao explorar a noção de complexidade dos algoritmos, os criadores dessas tecnologias promovem uma narrativa que os isenta da obrigação de prestar contas e de assumir

---

[170] A teoria mencionada é da regulação responsiva que possui como premissa a concepção de que uma política regulatória satisfatória "trata de compreender a regulamentação privada - por associações da indústria, por empresas, por pares e por consciências individuais - e como ela é interdependente com a regulamentação estatal". [...] "A regulação responsiva trata principalmente de encontrar o equilíbrio certo entre punição e persuasão". PEREIRA, José Renato L. de. Transparência pela cooperação: como a regulação responsiva pode auxiliar na promoção de sistemas de *machine-learning* inteligíveis. *Revista de Direito Setorial e Regulatório*, v. 7, nº 1, p. 194-223, maio-junho 2021.

[171] WOLFGANG, Hoffmann-Riem. Desafios jurídicos no uso de dados, em especial no que diz respeito a big data e ia. In: WOLFGANG, Hoffmann-Riem. *Teoria Geral do Direito Digital*. São Paulo: Grupo Gen, 2021. p. 116-120. Disponível em: https://app.minhabiblioteca.com.br/#/books/9786559642267/. Acesso em: 28 set. 2023.

a responsabilidade por eventuais efeitos adversos de seus produtos, especialmente devido à opacidade inerente a essas tecnologias, caracterizada pelo termo "caixa preta".[172]

Em razão disso, há uma extensa discussão sobre o desenvolvimento de abordagens para compreender esses sistemas. São alguns exemplos de tais esforços: a condução de auditorias — sejam elas de governança, dos modelos de IA em si (após o treinamento dos dados, mas antes de sua utilização) ou de aplicações específicas desses modelos — emerge como um método viável e essencial para auxiliar na detecção de falhas e riscos dessas tecnologias.

Essas abordagens têm ilustrado que, de fato, é viável avaliar a conformidade legal de sistemas de inteligência artificial, mesmo quando não se consegue precisar exatamente o caminho que levou a um resultado específico. Assim, a transparência emerge como um princípio essencial que deve orientar a avaliação dessas tecnologias e deve ocorrer de maneira abrangente. Adicionalmente, é crucial que a legislação reflita a inclinação de que a transparência é relevante não apenas para compreender a operação técnica de um sistema, mas também para outras questões relacionadas ao seu desenvolvimento e implementação.[173]

O texto conta com uma série de recomendações ao texto legal do projeto em questão, mas que se fazem relevantes para qualquer outra legislação que busque regular o tema discutido. São elas: a) Direito à informação para sujeitos afetados; b) Adesão a código de boas práticas e de governança; c) Auditorias; d) Sistemas utilizados pelo poder público[174] e; e) Informações sobre impactos ambientais.[175]

No capítulo anterior, mencionamos como o Princípio da Inteligência Artificial Explicável pode configurar uma das respostas para os clamores relacionados à falta de transparência algorítmica e ao direito à explicação, de forma que dentro da lógica do mencionado princípio, a inclusão do ponto da transparência deve ser um componente essencial nos sistemas inteligentes, proporcionando confiança ao usuário. Ademais, é fundamental que os sistemas de inteligência artificial, especialmente aqueles que implicam riscos significativos, sejam considerados confiáveis.

---

[172] AZEVEDO, Cynthia Picolo Gonzaga de. BUARQUE, Gabriela. PEREIRA, José Renato Laranjeira de. *Nota Técnica ao Projeto de Lei nº 2338/2023.* Coalizão Direitos na Rede, agosto de 2023, p. 21-22.

[173] *Ibidem*.

[174] No contexto de criação, obtenção e utilização de inteligência artificial por órgãos públicos, é crucial que a clareza esteja ancorada na legislação de acesso à informação. Isso implica estabelecer uma lista de dados mínimos que seja assegurada ao público por meio de transparência ativa, não se limitando apenas ao usuário ou à "pessoa diretamente impactada".

[175] Os dados sobre a quantidade real de recursos que são utilizados ainda são inadequados para entender verdadeiramente a extensão do impacto ambiental associado ao ecossistema do desenvolvimento, operação e descarte desses sistemas. AZEVEDO, Cynthia Picolo Gonzaga de. BUARQUE, Gabriela. PEREIRA, José Renato Laranjeira de. *Nota Técnica ao Projeto de Lei nº 2338/2023*. Coalizão Direitos na Rede, agosto de 2023, p. 23-35.

Retomando tais conceitos, fundamental refletir sobre a possibilidade de falhas das tecnologias aqui debatidas, uma vez que, independentemente de sua sofisticação, um sistema de inteligência artificial não está isento de gerar resultados imprecisos, incompletos ou tendenciosos, diversos motivos podem estar por trás de uma previsão incorreta.

Os dados de entrada podem ser incompletos ou conflitantes, criando ambiguidades para o algoritmo que os analisa. Adicionalmente, a previsão computacional pode estar inadequadamente calibrada ou insuficientemente treinada, resultando em uma interpretação inadequada desses dados e, consequentemente, em resultados incorretos. Por fim, existem casos nos quais o algoritmo "acerta" a resposta, mas recorre a raciocínios e aproximações indesejáveis.[176]

A falha acontece quando um sistema não consegue correlacionar os dados de maneira causal, resultando em evidências inconclusivas e ações sem justificativa. Um exemplo se dá quando algoritmos classificadores de imagens se confundem ao tentar diferenciar entre lobos e cães da raça Husky, especialmente em situações em que há neve na imagem.

Assim, quando um algoritmo gera uma decisão equivocada – ou mesmo correta, mas baseada em premissas falsas –, estamos diante da suscetibilidade a falhas, uma condição na qual o sistema de IA não opera conforme desejado, seja por questões relacionadas ao design do algoritmo ou pela maneira como os dados são codificados, coletados, selecionados ou empregados no treinamento do algoritmo.[177]

Ainda que o foco aqui seja refletir acerca dos direitos dos usuários, o grau de minúcia e as propriedades da Inteligência Artificial Explicável devem ser definidos considerando o público destinatário da explicação. É fundamental, portanto, que seu avanço não perca de vista o seu usuário final, devendo disponibilizar, conforme o destinatário, a quantidade adequada de informações e explicações em linguagem compreensível para o interlocutor.

Desta forma, a explicação não deve caracterizar mera formalidade ou enunciado de normas, mas interpretações coerentes das práticas ou estrutura do sistema. Uma declaração formal de "por que optamos por essa abordagem" é uma justificativa, não uma explicação.[178] Evidente que considerando aplicações de "*machine learning*" este procedimento se torna mais complexo e esbarra inevitavelmente na opacidade tão mencionada ao longo deste trabalho e demais textos relacionados ao assunto.

---

[176] ALVES, Marco Antônio Sousa; DE ANDRADE, Otávio Morato. Da "caixa-preta" à "caixa de vidro": o uso da *explainable artificial intelligence* (XAI) para reduzir a opacidade e enfrentar o enviesamento em modelos algorítmicos. *Direito Público*, v. 18, n. 100, 2021.
[177] *Ibidem*.
[178] *Ibidem*.

Além das implicações já mencionadas sobre este desafio, como confiabilidade do usuário e aperfeiçoamento dos modelos, há também a conformidade legal. Uma vez que a regulação tem sido uma pauta frequente em discussões públicas, se faz fundamental ponderar sobre o grau de conformidade disponível em tais tecnologias. Nesse contexto, mesmo que a inteligência artificial proporcione notáveis oportunidades em nossa vida diária, é consenso entre os especialistas no assunto que sua falta de transparência, em determinadas situações, não é preferível.

O papel do princípio em questão será crucial para compreender, analisar e retificar esses sistemas, buscando continuamente assegurar sua conformidade ética e legal. Para Alves e Andrade, entretanto, nem todo sistema de inteligência artificial pressupõe a aplicação da explicabilidade. Os autores citam como exemplos situações em que o modelo algorítmico e suas predições têm baixo impacto, não havendo desdobramentos sociais, e em um cenário no qual as utilizações de um sistema específico já estejam devidamente examinadas e consolidadas, como ocorre na situação em que o reconhecimento facial é empregado para o desbloqueio de dispositivos móveis.[179]

Sobre tais considerações, ressaltamos que embora as proposições possam ser adotadas, isto não implica em redução dos demais direitos do usuário resguardados por outras legislações como a LGPD, a Lei de Acesso à Informação e a Lei do Cadastro Positivo, por exemplo.

A literatura técnica estabelece uma diferenciação entre modelos algorítmicos que são intrinsecamente interpretáveis e aqueles que precisam ser elucidados por meio de técnicas específicas de Explicabilidade em Inteligência Artificial. Um modelo de aprendizado de máquina "transparente" é aquele que é autoexplicativo, não necessitando de métodos adicionais para que as pessoas possam entendê-lo. Também existem os "modelos opacos", cujo entendimento requererá um processo adicional de explicação, conhecido como esclarecimento pós-análise. Este utiliza várias estratégias, como interpretações de texto, representações visuais, exemplificações, simplificações e análises de relevância de recursos.[180]

Nesse sentido, para Vieira e Digiampietri, a forma mais simples de atingir a explicabilidade é empregar apenas um conjunto de algoritmos que produzem modelos compreensíveis. Regressão linear, regressão logística e a árvore de decisão são frequentemente

---

[179] ALVES, Marco Antônio Sousa; DE ANDRADE, Otávio Morato. Da "caixa-preta" à "caixa de vidro": o uso da *explainable artificial intelligence* (XAI) para reduzir a opacidade e enfrentar o enviesamento em modelos algorítmicos. *Direito Público*, v. 18, n. 100, 2021.

[180] *Ibidem*. Em relação à estratégia da relevância de recursos os autores deliberam que tem como propósito elucidar mais detalhadamente um algoritmo não transparente, destacando os elementos e variáveis críticos para o resultado da previsão algorítmica.

categorizados como modelos interpretáveis. Contudo, a grande desvantagem é a diminuição do desempenho preditivo em comparação com outros modelos de aprendizado de máquina, além da restrição a alguns tipos de modelos.

Uma alternativa é utilizar métodos de interpretação específicos para cada tipo de modelo. A desvantagem disso é que há o risco da restrição a um tipo de modelo e pode ser desafiador mudar. Como opção a essas abordagens, há a separação das explicações do modelo de aprendizado de máquina (métodos de interpretação independentes do modelo).

A principal vantagem dos métodos de interpretação que não dependem do modelo em comparação com aqueles específicos para cada modelo é a versatilidade. Os criadores de aprendizado de máquina têm a liberdade de escolher qualquer modelo de aprendizado de máquina, pois os métodos de interpretação podem ser utilizados em qualquer modelo. Qualquer elemento que se apoie em uma interpretação de um modelo de aprendizado de máquina, como um gráfico ou interface de usuário, também adquire independência em relação ao modelo de aprendizado de máquina subjacente.[181]

Diante das exposições acima, é possível argumentar que a proposta de utilizar métodos de interpretação específicos para cada tipo de modelo pode levar a uma restrição significativa. Isso pode dificultar a adaptação a modelos diferentes, limitando a flexibilidade dos desenvolvedores, assim como a ideia de empregar apenas algoritmos que produzem modelos compreensíveis, como regressão linear e árvore de decisão, pode limitar a complexidade dos modelos, resultando em perda de desempenho preditivo em comparação com modelos mais avançados.

Dessa forma, nos vemos novamente perante o embate entre inovação/avanços tecnológicos e transparência/direitos. No entanto, é essencial que a solução envolva uma análise mais aprofundada e uma abordagem equilibrada entre explicabilidade e desempenho preditivo no desenvolvimento de sistemas de IA eficientes.

Comumente, não apenas um, mas uma variedade de modelos de aprendizado de máquina é examinada para enfrentar uma determinada tarefa. Ao realizar comparações de modelos em termos de explicabilidade, é mais vantajoso empregar explicações que não estejam vinculadas ao modelo específico, uma vez que esse mesmo método pode ser empregado em qualquer classe de modelo.

---

[181] VIEIRA, C. P. R.; DIGIAMPIETRI, L. A. A study about Explainable Articial Intelligence: using decision tree to explain SVM. *Revista Brasileira de Computação Aplicada*, v. 12, n. 1, p. 113-121, 2020. Disponível em: https://seer.upf.br/index.php/rbca/article/view/10247. Acesso em: 29 out. 2023.

Os autores também listam os principais obstáculos para desvendar um algoritmo de caixa-preta. Classificam-nos de maneira a identificar pequenos elementos distintivos nas abordagens de explicação, como, por exemplo, árvore de decisão em comparação com árvore única, SVM, entre outros. São analisadas quatro características para cada método de explicação: a) A natureza do problema enfrentado; b) A capacidade explicativa empregada para elucidar a caixa-preta; c) O tipo de modelo de caixa-preta que pode ser explicado; e d) Os tipos de dados de entrada fornecidos ao modelo de caixa-preta.[182]

O texto discutido anteriormente apresenta uma perspectiva clara sobre a variedade de modelos de aprendizado de máquina e a relevância da explicabilidade na análise comparativa desses modelos. A sugestão de utilizar esclarecimentos independentes do modelo é enfatizada como uma abordagem conveniente, ressaltando a desejável flexibilidade e generalização em métodos de explicação.

A listagem das principais complexidades para "revelar" um algoritmo de caixa-preta é valiosa, realçando a dificuldade intrínseca desse desafio. A categorização dessas complicações em pequenos elementos distintivos nas abordagens de explicação proporciona uma estrutura organizada para compreender os desafios associados.

Em relação a instrumentos para reduzir a opacidade, Bioni e Luciano, em publicação de 2019, avaliam a possibilidade de utilizar as leis de proteção de dados como um ponto de entrada para regulamentar a inteligência artificial. Além disso, o texto também faz uma análise crítica sobre o papel do princípio da precaução nesse contexto, discutindo questões éticas, regulatórias e de responsabilidade relacionadas à IA e ao direito.

Para a discussão em questão, precaução é compreendida conforme disposto na Declaração do Rio sobre Meio Ambiente e Desenvolvimento de 1992 (Rio 92), a qual uma estratégia de precaução deveria ser extensivamente utilizada pelos Estados, em conformidade com suas competências, visando à preservação do meio ambiente.[183]

---

[182] ALVES, Marco Antônio Sousa; DE ANDRADE, Otávio Morato. Da “caixa-preta” à “caixa de vidro”: o uso da *explainable artificial intelligence* (XAI) para reduzir a opacidade e enfrentar o enviesamento em modelos algorítmicos. *Direito Público*, v. 18, n. 100, 2021. Árvores de decisão são definidas como um exemplo de modelo que pode prontamente atender a todas as restrições para transparência. Essas estruturas hierárquicas para tomada de decisões são empregadas para respaldar problemas de regressão e classificação. Contudo, as características de generalização menos eficazes em comparação com outros modelos tornam essa categoria de modelos menos atrativa para sua implementação em contextos nos quais um equilíbrio entre o desempenho preditivo é um elemento crucial de design. Já os modelos SVM são mais complexos do que as árvores de decisão, apresentando uma estrutura significativamente mais opaca. De maneira simplificada a "Máquina de Vetores de Suporte" (SVM) é um algoritmo de aprendizado supervisionado que pode ser aplicado a problemas de classificação ou regressão. Sua ênfase recai sobre o treinamento e a categorização de um conjunto de dados.

[183] “Art. 15: In order to protect the environment, the precautionary approach shall be widely applied by States according to their capabilities. Where there are threats of serious or irreversible damage, lack of full scientific certainty shall not be used as a reason for postponing cost-effective measures to prevent environmental

Trata-se, portanto, de assumir compromissos com a deliberação e a responsabilidade, garantindo explicações explícitas e cuidadosas acerca das escolhas regulatórias realizadas diante de um "conhecimento incompleto" - algo que, de fato, estimularia e estabeleceria obrigações para com a pesquisa e o conhecimento científico, visando a obtenção de informações sobre os riscos desconhecidos.

Entender o princípio da precaução como uma forma de racionalidade a ser utilizada durante a seleção das medidas regulatórias aborda as principais objeções feitas à sua aplicação. A primeira delas aponta para a indeterminação de alguns dos termos utilizados nas formulações. Essa crítica assume que se trata de uma norma procedimental e auto-suficiente, o que o afastaria da própria concepção de princípio. A segunda crítica caracteriza o princípio como "não científico" e "irracional" devido ao seu alegado caráter normativo.[184]

Os autores respondem às respectivas críticas avaliando que estes parecem depositar uma confiança excessiva na convicção do conhecimento científico imparcial, presumindo que procedimentos regulatórios convencionalmente orientados pela ciência (e menos propensos à participação de diversos interessados, convém ressaltar) seriam capazes de superar essa normatividade e indeterminação.

Finalmente, a terceira objeção à implementação do princípio seria a sua recusa a novas tecnologias devido ao seu caráter "paralisante", priorizando medidas que encerrem ou dificultem o progresso tecnológico com determinações de "não-agir". Entretanto, a escolha de não adotar qualquer medida é apenas uma das opções dentro do contexto da precaução. O princípio concentra-se nas razões para tomar decisões regulatórias específicas, não nas decisões em si, além de avaliar o grau de envolvimento e participação do público nesses processos decisórios.[185]

A partir disso, têm a intenção de avaliar a sua proximidade em relação aos objetivos regulatórios e ao formato atual das leis de proteção de dados pessoais/LDPD. A noção de responsabilidade ("*accountability*") e os relatórios de impacto na proteção de dados pessoais, elementos fundamentais das LPDPs, apresentam-se como possíveis portas de entrada para a

---

degradation". Tradução livre: Art. 15: Com o objetivo de proteger o meio ambiente, a abordagem precaucionária deve ser amplamente aplicada pelos Estados de acordo com suas capacidades. Quando houver ameaças de danos sérios ou irreversíveis, a falta de plena certeza científica não deve ser utilizada como motivo para adiar medidas economicamente viáveis para prevenir a degradação ambiental.

[184] BIONI, Bruno Ricardo; LUCIANO, Maria. O princípio da precaução na regulação da inteligência artificial: seriam as leis de proteção de dados o seu portal de entrada. *In*: FRAZÃO, Ana; MULHOLLAND, Caitlin. *Inteligência artificial e direito:* ética, regulação e responsabilidade. São Paulo: Thomson Reuters Brasil, p. 207-232, 2019.

[185] *Ibidem*.

aplicação do princípio da precaução à IA especialmente considerando que grande parte do uso dessa tecnologia envolverá o processamento de dados pessoais.

Ocorreu e está ocorrendo uma mudança de paradigma na estrutura teórica no âmbito da proteção de dados. Enquanto anteriormente o sistema orbitava totalmente em torno da perspectiva da autodeterminação informacional, a sua órbita ocorre cada vez mais em torno dos processos de gestão dos riscos das atividades de tratamento de dados.

Não se trata de um processo de choque jurídico ou de substituição normativa, mas sim de uma nova classificação em relação à emergência de mecanismos mais focalizados na identificação e mitigação das incertezas e das probabilidades dos malefícios decorrentes da manipulação das informações pessoais dos indivíduos. Resumidamente, o resultado normativo das recentes legislações sobre proteção de dados pessoais decorre cada vez mais de uma estrutura precaucionária em relação a danos.[186]

Conforme discutido ao longo deste trabalho, a linha condutora de todo esse desenvolvimento é a intensificação da disparidade de informações, que, embora seja um componente histórico na formulação de leis de proteção de dados, atingiu um nível ainda mais elevado diante dos progressos tecnológicos e da consolidação de uma economia impulsionada e guiada por dados. Com isso, o processo de compreensão, análise e gestão dos riscos em uma economia de dados torna-se mais intrincado. Os agentes responsáveis pelo tratamento de dados – controladores e operadores – passaram a deter uma vantagem informacional ainda mais pronunciada em comparação com os demais participantes – cidadãos e órgãos fiscalizadores – desse ecossistema.[187]

Num cenário em que a proteção de dados é enfatizada de modo rigoroso, há o perigo potencial de criar obstáculos excessivos para a inovação. A evolução de tecnologias avançadas frequentemente demanda a coleta e análise de grandes quantidades de dados, e uma postura excessivamente cautelosa pode desencorajar empresas e pesquisadores de buscar soluções criativas devido ao receio de punições ou limitações regulatórias.

Portanto, é crucial encontrar um equilíbrio apropriado entre a proteção das informações pessoais e a fomentação da inovação. Isso pode incluir a implementação de medidas que viabilizem a inovação responsável, tais como a integração de princípios éticos no

---

[186] BIONI, Bruno Ricardo; LUCIANO, Maria. O princípio da precaução na regulação da inteligência artificial: seriam as leis de proteção de dados o seu portal de entrada. *In*: FRAZÃO, Ana; MULHOLLAND, Caitlin. *Inteligência artificial e direito:* ética, regulação e responsabilidade. São Paulo: Thomson Reuters Brasil, p. 207-232, 2019.
[187] *Ibidem*.

desenvolvimento de tecnologias, a transparência no uso de dados e a cooperação entre os setores público e privado para estabelecer diretrizes regulatórias equilibradas.

Nessa situação, o princípio da responsabilidade ("*accountability*") surge como um vetor crucial para a abertura dos procedimentos de tomada de decisão sobre o que será considerado um risco aceitável nas operações de tratamento de dados. Isso ocorre porque a participação e o envolvimento do público nessas instâncias decisórias serão diretamente proporcionais à flexibilidade do conteúdo dessa obrigação de prestação de contas por parte dos agentes econômicos.[188]

À medida que grande parte das decisões automatizadas com o uso de inteligência artificial incluirá o tratamento de dados pessoais, normativas amplas de proteção de dados, formuladas com base em uma perspectiva de regulação de risco e no princípio da responsabilidade, constituem elementos que democratizam o próprio procedimento de regulamentação dessa tecnologia.

Os Relatórios de Impacto à Proteção de Dados Pessoais (RIPDP) têm adquirido uma posição cada vez mais proeminente nas legislações voltadas para a proteção de dados pessoais. De maneira geral, tais documentos seriam o registro pelo qual o responsável - aquele que detém a autoridade decisória na cadeia de manipulação de dados - documentaria seus procedimentos de manipulação de dados e as medidas adotadas para atenuar os riscos gerados aos direitos dos titulares dos dados.

Na realidade brasileira, a legislação geral de proteção de dados pessoais não sistematizou de maneira mínima o RIPDP. Apesar de existirem algumas referências a esse instrumento, não há um capítulo específico para abordar o assunto. Dessa forma, o RIPDP estaria sujeito à regulamentação posterior por parte de órgãos fiscalizadores que precisariam definir quando seria compulsório, bem como quais elementos e o tipo de análise que se espera encontrar nesse documento.[189]

Dessa forma, mais uma potencial abordagem para a implementação do princípio da precaução na regulamentação da inteligência artificial são os documentos de avaliação de impacto à proteção de dados pessoais, conforme estabelecidos em leis de proteção de informações pessoais. No entanto, a intensidade com que esse princípio é efetivamente aplicado pode variar por meio dessa ferramenta, especialmente no que diz respeito à avaliação do risco

---

[188] BIONI, Bruno Ricardo; LUCIANO, Maria. O princípio da precaução na regulação da inteligência artificial: seriam as leis de proteção de dados o seu portal de entrada. *In*: FRAZÃO, Ana; MULHOLLAND, Caitlin. *Inteligência artificial e direito*: ética, regulação e responsabilidade. São Paulo: Thomson Reuters Brasil, p. 207-232, 2019.

[189] *Ibidem*.

resultando em ações ou inações por parte do proponente da tecnologia ao introduzi-la no ambiente.

O princípio da precaução, ao lidar com os perigos e desconhecimentos relacionados à inteligência artificial, enfatiza a relevância de contemplar duas estratégias regulatórias. Inicialmente, a imperatividade de instaurar a discussão regulatória para todos os intervenientes na incorporação da tecnologia, desde os criadores até aqueles afetados por suas consequências, fomentando a participação democrática e abordando as históricas dinâmicas de assimetria de poder e informação. Em segundo plano, realça a importância de impor responsabilidades para diminuir as incertezas acerca dos benefícios e riscos da IA determinando se ela deve ser adotada ou não.

As medidas relacionadas na parte final deste ponto constituem exemplos de como reduzir a opacidade de maneira preventiva. Além disso, as leis gerais de proteção de dados pessoais, bem como leis setoriais relacionadas a dados biométricos e reconhecimento facial, oferecem ferramentas a serem consideradas para contribuir na tarefa.

Ao longo deste capítulo discutimos o conceito de dado pessoal, desde sua origem ligado ao direito de privacidade (que obteve destaque na doutrina moderna após o artigo de Warren e Brandeis), passando pela Lei Geral de Proteção de dados (LGPD), e chegando ao seu reconhecimento como direito fundamental.

A privacidade foi inicialmente concebida na ideia do direito a ser deixado só, ou seja, uma definição a partir da negação do acesso do outro a determinados espaços privados. Esta sofreu diversas transformações até adotar uma concepção positiva, associada ao estado de bem-estar social (que ampliou a perspectiva da população acerca deste direito, assim como alavancou sua importância perante a sociedade de modo geral e não apenas de uma parcela específica).

As mudanças estruturais e tecnológicas deixaram claro que proteger apenas a privacidade não era mais suficiente, frente a uma era de processamento de dados em massa, tal qual a que estamos inseridos. Dessa forma, manifestou-se a necessidade do direito à proteção de dados como autônomo, posteriormente, este teve sua importância reconhecida como ainda mais elevada, sendo identificado como direito fundamental. Tal caracterização é fruto de uma transição reconhecida pelos três Poderes da República (a decisão do STF no caso do IBGE/2020; a proposta de Emenda Constitucional aprovada nas Casas Legislativas e a sanção presidencial da referida PEC).

Nesse sentido, os dados pessoais não apenas representam informações sobre uma pessoa, mas funcionam como uma extensão dela, desempenhando um papel fundamental na capacidade dessa pessoa desenvolver sua personalidade de maneira livre e autêntica. Essas

informações, quando gerenciadas com responsabilidade e respeito à privacidade, proporcionam um ambiente no qual o indivíduo pode explorar suas características, preferências e experiências, contribuindo assim para o enriquecimento e a expressão genuína de sua identidade. Portanto, reconhecer a importância dos dados pessoais implica não apenas em respeitar a privacidade, mas também em valorizar a autonomia e a liberdade individual na formação e evolução da personalidade.

Em seguida, apresentamos alguns exemplos de implicações da coleta e tratamento de dados em nosso cotidiano. Tais como: o caso da "Cambridge Analytica" e o relatório "*Human rights, democracy and the rule of law assurence framework for AI systems*", elaborado pelo Instituto Alan Turing. Abordamos também casos dentro da administração pública, como apontados em relatório da Transparência Brasil, a ferramenta Bem-te-vi, utilizada pelo Tribunal Superior do Trabalho, e a plataforma Victor, aplicada no Supremo Tribunal Federal.

Durante a segunda parte deste capítulo, debatemos as formas de tratamento de dados e revisão de decisões automatizadas, de forma que definimos a última como aquela que é assim caracterizada quando conduzida com referência a dados individuais manipulados de forma artificial por meio de algoritmos, resultando na formulação de conjuntos de dados organizados ou "criação de perfis", habilitando a realização de análises e previsões (por seres humanos ou inclusive por máquinas) sobre comportamentos e até mesmo atitudes morais da pessoa envolvida.

Nesse cenário, é crucial destacar a ilusão equivocada de que, ao não depender da intervenção humana na tomada de decisões, as tecnologias em destaque seriam inerentemente imparciais ou isentas de equívocos. A partir dessa observação, podemos inferir que o desafio não reside na capacidade da inteligência artificial cometer erros, mas sim na habilidade dela em nos persuadir de que a ocorrência de falhas é inconcebível.

A confiança cega na infalibilidade dessas tecnologias pode, de fato, obscurecer a compreensão crítica necessária para lidar com as implicações e limitações intrínsecas aos sistemas automatizados. Portanto, é essencial manter uma perspectiva consciente e questionadora em relação à confiabilidade das soluções baseadas em inteligência artificial, promovendo uma abordagem mais informada e responsável no seu desenvolvimento e implementação.

Definimos a prática de "*profiling*" como a que envolve a construção de perfis comportamentais com base em dados fornecidos ou coletados de uma pessoa, sendo realizada por meio de métodos estatísticos e técnicas de inteligência artificial. Essas informações são

processadas com o objetivo de obter "metainformações", que abrangem a compilação de padrões, preferências pessoais e outros registros da vida do indivíduo.

Considerando a conceituação acima, debatemos determinadas características distintivas da perfilagem devido ao procedimento automatizado conduzido por algoritmos. Isso inclui a falta de determinação das causas ou motivos por trás das relações identificadas, a correspondência da precisão do processo com a quantidade de dados coletados, tornando problemático o princípio da minimização de dados e a disparidade informacional entre o titular dos dados e o controlador.

A partir dessas considerações, é possível concluir que a assimetria de poder entre o titular e as empresas ou entidades governamentais que detêm tecnologias de processamento em massa é acentuada pela escassez de informações.

De mesmo modo, "*data mining*", se refere à extração não trivial de informações úteis a partir de conjuntos de dados, indo além da simples coleta de dados organizados. Esse processo pode ser automatizado ou semiautomatizado, visando identificar padrões significativos nos dados para adquirir informações relevantes e apoiar a criação de conhecimento.

O desafio reside na possibilidade de simplificação excessiva, negligenciando aplicações benéficas da tecnologia. Destaca-se a importância de não encarar as informações individuais como uma "fonte inesgotável" para uso irrestrito no universo digital, alertando contra o risco de explorar dados apenas visando ganhos financeiros, sem considerar outros propósitos e interesses protegidos.

Apontamos as implicações do tratamento de dados nos direitos à privacidade e proteção de dados, destacando que a criação de uma imagem virtual pode impactar a liberdade e personalidade de uma pessoa. O direito à transparência é enfatizado como crucial para garantir que os indivíduos tenham conhecimento e controle sobre a coleta e uso de seus dados, promovendo equidade na era da tecnologia.

É ressaltada a necessidade de operações alinhadas com os critérios de proteção da dignidade humana estabelecidos pelos direitos fundamentais, com mecanismos que permitam controle eficaz sobre informações individuais, assegurando acesso, veracidade, segurança e compreensão de sua finalidade.

No ponto final, mencionamos a importância da transparência algorítmica e interpretabilidade global para compreender como os algoritmos processam dados e as relações resultantes. Essa compreensão é vital para regular a inteligência artificial. A necessidade de diferentes formas de esclarecimentos atender a grupos variados, incluindo usuários e legisladores, ressalta a complexidade da regulação da IA.

A perspectiva do usuário, com suas diversas necessidades, destaca a importância de um acesso facilitado às informações, o que pode ser um elemento crucial na elaboração de políticas regulatórias que equilibrem os interesses das empresas e a transparência exigida para a *accountability* e a confiança na adoção da IA. O respeito aos direitos de propriedade intelectual e industrial é mencionado como uma consideração importante ao conceder esse acesso. Portanto, destacamos aspectos fundamentais para a regulação da IA abordando transparência e interpretabilidade, outros fatores serão abordados no próximo capítulo.

3. ANONIMIZAÇÃO E PROTEÇÃO DE DADOS EM INTELIGÊNCIA ARTIFICIAL: DESAFIOS, REIDENTIFICAÇÃO E MARCO REGULATÓRIO

3.1 O PAPEL DA ANONIMIZAÇÃO NA PROTEÇÃO DE DADOS NO CONTEXTO DA IA

A anonimização é um procedimento essencial para resguardar a privacidade e a segurança das informações pessoais em contextos digitais, consistindo na conversão de dados identificados ou identificáveis em dados não identificáveis e evitando que pessoas sejam prontamente reconhecidas com base nesses dados.

Além de salvaguardar a privacidade dos indivíduos, a anonimização também desempenha um papel fundamental na promoção da pesquisa e inovação em diversas áreas, pois, ao permitir o uso de dados para análises estatísticas e pesquisas científicas sem a preocupação de violar a privacidade, ela estimula o avanço do conhecimento e o desenvolvimento de novas soluções.[190]

Essas metodologias tornaram-se fundamentais para assegurar a segurança das informações em extensas bases de dados, oferecendo alternativas eficazes para preservar a identidade das pessoas representadas nos dados. A implementação de normas rigorosas, como a GDPR, em 2018, aumentou consideravelmente a importância da anonimização, e hoje, as organizações são legalmente compelidas a tornar anônimos dados pessoais para resguardar a privacidade das pessoas, o que destaca a exigência de técnicas de anonimização eficazes e robustas.

A GDPR estabeleceu regulamentações precisas sobre o uso e a salvaguarda de dados pessoais, delineando orientações tangíveis sobre a necessidade de anonimização para proteger a privacidade dos indivíduos. A anonimização tornou-se não apenas uma boa prática, mas muitas vezes uma exigência legal. O mesmo ocorreu com a LGPD, por exemplo, que no artigo 5º, inciso XI define anonimização como "[...] utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo".

Este procedimento desempenha um papel vital em garantir a conformidade com regulamentações de privacidade, como o GDPR na União Europeia e outras leis semelhantes ao redor do mundo. De acordo com o Instituto Avançado de Proteção de Dados (IAPD), a

[190] BIONI, Bruno. Compreendendo o conceito de anonimização e dado anonimizado. *Cadernos Jurídicos*. São Paulo, v. 21, p. 191-201, 2020.

anonimização representa um mecanismo essencial para proteger a privacidade humana, eliminando qualquer ligação que possa identificar um dado com seu respectivo proprietário, processo que utiliza meios técnicos disponíveis no momento do tratamento de dados pessoais, assegurando que nenhum dado esteja vinculado diretamente ou indiretamente a seu titular.[191]

Esse direito, garantido pelo artigo 18, IV, da LGPD, não apenas permite que os titulares de dados pessoais evitem o uso indevido de informações consideradas desnecessárias ou excessivas, mas também exige a aplicação da anonimização sempre que possível, especialmente ao lidar com dados pessoais e sensíveis, conforme estabelecido nos artigos 7º, inciso IV, e 11 da LGPD, respectivamente.

Conforme mencionado, a anonimização conduz à geração de informações desidentificadas, que representam a antítese das informações de natureza pessoal. Estas últimas referem-se a dados que não possuem a capacidade de revelar a identidade de um indivíduo, e, por conseguinte, não demandam as mesmas salvaguardas legais.

A obtenção de dados desidentificados compreende práticas como a randomização, que modifica a autenticidade dos dados introduzindo variação ou permutação para eliminar associações intensas com o detentor dos dados, e a generalização, que ajusta a ordem de grandeza dos dados, tornando as informações menos pormenorizadas com o intuito de romper os laços de identificação.[192]

Além disso, algumas técnicas, como a pseudoanonimização, são discutidas, embora haja cautela devido à possibilidade de reversão dos dados anonimizados, conforme observado na Lei Geral de Proteção de Dados Pessoais.

A ideia da anonimização é dificultar a ponto de tornar impossível associar os dados a uma pessoa específica. O processo é concebido mirando em ser irreversível, entretanto, com os avanços tecnológicos caminhando em uma velocidade cada vez mais alta, alcançar este fim tem se tornado cada vez mais desafiador. Nesta orientação, é o que indica Bioni:[193]

> Com maior ou menor grau de intensidade nota-se um método cujo mote é gerenciar circunstancialmente a identificabilidade de uma base de dados. As características de cada dado e a percepção de eles estarem inseridos em uma gama de informações devem orientar tal análise. Por isso, não há um único método ou uma combinação perfeita ex ante para parametrizar o processo de anonimização, devendo-se analisar contextualmente como este deve ser

---

[191] POSSI, Ana Beatriz Benincasa Possi Benincasa. *O Que é Anonimização e Pseudoanonimização De Dados?* Instituto Avançado de Proteção de Dados, 2 de novembro de 2019. Disponível em: https://iapd.org.br/o-que-e-anonimizacao-e-pseudoanonimizacao-de-dados/. Acesso em: 23 out. 2023.

[192] BIONI, Bruno. Compreendendo o conceito de anonimização e dado anonimizado. *Cadernos Jurídicos*. São Paulo, v. 21, p. 191-201, 2020.

[193] BIONI, Bruno. Compreendendo o conceito de anonimização e dado anonimizado. *Cadernos Jurídicos.* São Paulo, v. 21, p. 191-201, 2020.

> empreendido para que os titulares dos dados anonimizados não sejam reidentificados, nem mesmo por quem procedeu à sua anonimização.

Conforme mencionado nos capítulos anteriores desta exposição, antes da era digital transformar a maneira como vivíamos e interagíamos com informações, preocupações como a anonimização eram extremamente limitadas. A coleta e o armazenamento de dados ocorriam principalmente em formato físico e a ênfase estava na segurança física dos documentos.

Entretanto, diante do advento de todos os progressos detalhados desde os primórdios da computação, as inquietações acerca da privacidade começaram a expandir de maneira acentuada. Apesar de terem sido concebidas técnicas criptográficas, a efetiva anonimização tornou-se uma dificuldade considerável devido à elevação exponencial na quantidade de dados ("*big data*").

A necessidade de tornar anônimos os dados, alcançou níveis inéditos com o crescimento das aplicações aqui debatidas e o aumento substancial da coleta de informações *online*, e para enfrentar essa dificuldade técnicas avançadas como generalização (agregação de dados), supressão (remoção de dados) e substituição (troca de valores) foram desenvolvidas.[194]

Por generalização podemos compreender converter os dados em faixas, assegurando uma visão global e abrangente de cada entrada. Claramente, é mais simples fazer generalizações com dados numéricos. No caso dos textos, o desafio é ampliado. Do mesmo modo, alguns dados numéricos, como os registros de CPF, não podem ser prontamente generalizados.

Dados como "idade exata", por exemplo, podem ser generalizados para faixas etárias, como crianças, adolescentes, adultos jovens, adultos e idosos. Da mesma forma, localizações precisas podem ser generalizadas para regiões mais amplas, como países, estados ou cidades, processo que torna os dados menos precisos, mas ainda úteis para análises estatísticas e padrões gerais.

Dessa forma, a agregação é uma maneira de generalização que converte os dados em resumos, com menos entradas, através da normalização e do agrupamento de semelhantes. Em outras palavras, modifica-se a tabela para exibir os dados de maneira diferente. Esta se distingue da generalização convencional, pois efetivamente altera os dados, enquanto generalizar não implica necessariamente uma modificação ativa, mas apenas uma configuração simples em cada entrada.[195]

---

[194] MACHADO, Diego; DONEDA, Danilo. Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados. *Revista dos Tribunais*. vol. 998. Caderno Especial. p. 99-128. São Paulo: Ed. RT, dezembro 2018.

[195] COUTTO FILHO, Milton B. do; SOUZA, Julio C. Stacchini de; SCHILLING, Marcus T. Sobre o problema da integração generalizada de dados. *Sba:* Controle & Automação Sociedade Brasileira de Automatica, v. 18, n. 1, p. 24-43, mar. 2007. Disponível em: http://dx.doi.org/10.1590/s0103-17592007000100003. Acesso em: 23 out. 2023.

Outra abordagem, possivelmente mais direta, é a supressão de dados. Envolve a exclusão dos campos de dados que podem facilitar a identificação de pessoas. Em outras palavras, no conjunto de dados, são removidas as colunas associadas a informações distintas, como CPF, RG, nome completo, entre outras.[196]

É necessário exercer cautela ao utilizar essa estratégia, pois, mesmo com a supressão, ainda é possível recuperar algumas informações da tabela e, dessa forma, identificar uma pessoa. Por outro lado, apesar de se inferir que seja efetiva na preservação da privacidade, a supressão excessiva pode levar à perda de informações significativas, comprometendo assim a utilidade do conjunto de dados para análises.

Finalmente, a substituição consiste na reposição aleatória de conteúdo por informações não relacionadas ao dado real.[197] Nomes próprios, por exemplo, podem ser substituídos por "Usuário 1", "Usuário 2", etc., ou por identificadores únicos não relacionados aos dados reais. Da mesma forma, números de cartões de crédito podem ser substituídos por números fictícios, e datas de nascimento precisas podem ser substituídas por anos ou faixas de anos, ou seja, a substituição preserva a estrutura dos dados, mas altera os valores específicos para proteger a identidade dos indivíduos.

Apesar disto, torna-se cada vez mais frequente a divulgação de pesquisas com o intuito de expor as fragilidades nos procedimentos relacionados ao fenômeno da anonimização, buscando questionar a premissa de uma anonimização resistente.[198] Em contrapartida, técnicas algorítmicas sofisticadas estão sendo utilizadas para assegurar a proteção dos dados em contextos cada vez mais intrincados, oferecendo, dessa maneira, uma camada extra de salvaguarda contra ameaças contemporâneas à privacidade.

Necessário mencionar que ainda que a anonimização não seja revertida por vias tecnológicas, conforme debatido acima, persiste um perigo residual para os indivíduos mencionados nesses dados. O que acontece porque, mesmo que os dados não exponham diretamente a identidade de uma pessoa específica, outras fontes, sejam públicas ou privadas, podem ser empregadas para desfazer o processo de anonimização, fenômeno reconhecido como efeito mosaico.

O efeito mosaico é comparável a montar um quebra-cabeça com peças inicialmente desconexas; à medida que mais elementos são acrescentados, a imagem se torna mais nítida e

---

[196] FERREIRA, Juliano Rodrigues *et al*. Mitigação dos Riscos à Privacidade através da Anonimização de Dados. *Revista Ibérica de Sistemas e Tecnologias de Informação*, n. E49, p. 573-585, 2022.
[197] *Ibidem*.
[198] BIONI, Bruno. Compreendendo o conceito de anonimização e dado anonimizado. *Cadernos Jurídicos*. São Paulo, v. 21, p. 191-201, 2020.

elucidativa. Detalhes como idade, gênero, localização geográfica aproximada e preferências específicas podem não ser adequados para identificar singularmente uma pessoa. Contudo, ao amalgamar essas informações com dados provenientes de plataformas de redes sociais, registros de transações, históricos médicos ou outras compilações de informações acessíveis, a identidade de um indivíduo pode ser estabelecida com uma precisão notavelmente alta.[199]

Esse perigo remanescente é uma inquietação em termos de privacidade e segurança de dados, dado que mesmo a divulgação de informações aparentemente não identificáveis pode resultar na exposição de dados sensíveis e pessoais. Logo, esses dados não podem ser meramente tratados como informações não vinculadas a uma pessoa específica. Para ser genuinamente anônimo, os dados não devem possuir qualquer conexão permanente e irrevogável com uma pessoa identificável.[200]

Nesse sentido, retomando a ideia de pseudoanonimização apresentada inicialmente, esta, conforme artigo 13, §4º da LGPD consiste no "[...] o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro".

Uma avaliação desse mecanismo revela que a pseudonimização representa uma forma de alteração de dados pessoais, de modo que os dados pseudonimizados não formam uma categoria adicional de dados e não devem ser confundidos com dados tornados anônimos. Isso ocorre porque a pseudonimização inclui a substituição de identificadores diretos (como nomes ou números de identificação) por identificadores indiretos ou pseudônimos, o que implica que os dados pessoais são modificados de uma maneira que dificulta a identificação direta dos indivíduos, mas ainda permite a associação dos dados aos indivíduos originais por meio de informações adicionais armazenadas separadamente.

A pseudoanonimização, em termos simples, é uma técnica que camufla a identidade ao substituir um atributo por outro, de modo que, durante esse procedimento, dados pessoais são manipulados de tal forma que não podem mais ser diretamente associados ao seu detentor original, a menos que informações correlatas adicionais sejam consultadas. Esses dados adicionais são mantidos de forma independente e estão sujeitos a procedimentos técnicos e organizacionais rigorosos para assegurar que a informação pessoal permaneça dissociada de

---

[199] BIONI, Bruno. Compreendendo o conceito de anonimização e dado anonimizado. *Cadernos Jurídicos*. São Paulo, v. 21, p. 191-201, 2020.

[200] MACHADO, Diego; DONEDA, Danilo. Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados. *Revista dos Tribunais*. vol. 998. Caderno Especial. p. 99-128. São Paulo: Ed. RT, dezembro 2018.

seu titular.[201] Isso assegura a privacidade dos indivíduos, ao mesmo tempo em que preserva a integridade e a utilidade dos dados para fins legítimos.

De modo geral, criptografia é a arte de escrever de forma secreta com a finalidade de ocultar o significado de uma mensagem. As várias técnicas criptográficas contemporâneas que compõem o dispositivo de confidencialidade na segurança computacional, quando empregadas, codificam informações de tal maneira que somente o destinatário da comunicação ou o possuidor de chave criptográfica (seja simétrica ou assimétrica) pode ter acesso e compreender o conteúdo informativo.[202]

Para os autores, dados criptografados não equivalem a dados anônimos ou anonimizados apenas pelo fato de serem submetidos a uma operação de cifragem. Nesse sentido, este texto é dividido em duas seções: inicialmente, serão estabelecidos alguns parâmetros introdutórios sobre a definição de dado pessoal, dada a sua relevância hermenêutica na aplicação das leis de proteção de dados pessoais, bem como a sua posição em relação a dados pseudonimizados e dados anônimos.

Em seguida, é necessário confrontar as características das técnicas criptográficas implementadas nas tecnologias digitais contemporâneas com aquelas que efetivamente configuram a anonimização de dados, a fim de, juntamente com outros subsídios conceituais e dogmáticos, fornecer *insights* sobre o(s) estatuto(s) jurídico(s) aplicável(is) no Brasil aos dados pessoais criptografados.[203]

A diferenciação crucial entre dados criptografados e dados anonimizados possui consequências práticas relevantes no âmbito da proteção de dados e respeito à privacidade. Embora a codificação proporcione uma camada suplementar de resguardo, ela não assegura anonimização total. A compreensão dessa disparidade é essencial para conceber estratégias eficazes na preservação de dados.

Da mesma forma, a mera implementação da criptografia não elimina todos os perigos de identificação. Incidentes de violações de segurança, investidas avançadas ou mesmo incidentes involuntários de vazamento podem revelar dados codificados. Por conseguinte, as instituições necessitam adotar abordagens abrangentes que englobem não exclusivamente uma criptografia robusta, mas também levem em consideração outros componentes de segurança, como regulação de acesso, monitoramento contínuo e políticas de gestão de dados.

---

[201] MACHADO, Diego; DONEDA, Danilo. Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados. *Revista dos Tribunais.* vol. 998. Caderno Especial. p. 99-128. São Paulo: Ed. RT, dezembro 2018.
[202] *Ibidem*.
[203] *Ibidem*.

Há dois sistemas de criptografia de dados reconhecidos: criptografia de chave única (uma chave) e criptografia de chave dupla (duas chaves inter-relacionadas). Na realidade, a opção por métodos de criptografia de chave dupla, como RSA, DSA ou ECC, que empregam duas chaves - uma pública e outra privada, intensifica a segurança da informação.

Para além dessas técnicas criptografadas, temos a computação segura multipartida, que está sendo implementada em estratégias de aprendizado de máquina que resguardam a privacidade. Essas possibilitam a tornar anônimos os dados utilizados no treinamento/derivação do modelo, o próprio modelo derivado, e na fase de consulta.[204]

Desse modo, tokenização é uma estratégia não matemática para salvaguardar dados em repouso que substitui informações sensíveis por equivalentes não sensíveis. Essa abordagem não modifica a natureza ou extensão dos dados, sendo compatível com sistemas herdados, como bancos de dados que podem ser sensíveis ao comprimento e tipo de dados, mantendo, assim, a informação sensível oculta.

Como exemplo, a tokenização pode ser empregada na segurança de transações móveis, protegendo credenciais de pagamento ao substituí-las por um número gerado aleatoriamente que se assemelha ao número de conta primária do cliente, sendo que somente o banco processador de pagamento pode decifrar o dado de volta.[205]

Em relação ao trecho acima, fundamental ressaltar que a afirmação de que a tokenização é uma "estratégia não matemática" pode ser um pouco ambígua, pois todas as técnicas de criptografia, incluindo a tokenização, são fundamentadas em princípios matemáticos. Essa caracterização pode levar a uma interpretação equivocada sobre a natureza da tokenização.

Além disso, embora seja verdade que a tokenização mantém o formato geral dos dados, a substituição de informações sensíveis por equivalentes não sensíveis pode, em alguns casos, resultar em perda de informação ou contextos específicos. Por fim, dependendo da implementação, alguns sistemas de tokenização permitem a reversão, o que pode representar um risco em potencial.

O crescente entendimento acerca da confidencialidade das informações e as ameaças à integridade dos dados continuam a impulsionar a inovação em técnicas de pseudonimização. As organizações estão incessantemente desenvolvendo e aprimorando métodos para assegurar que os dados pessoais sejam pseudonimizados de maneira eficiente e segura.

---

[204] FERREIRA, Juliano Rodrigues et al. Mitigação dos Riscos à Privacidade através da Anonimização de Dados. *Revista Ibérica de Sistemas e Tecnologias de Informação*, n. E49, p. 573-585, 2022.
[205] *Ibidem*.

A pseudonimização desempenha uma função crucial na preservação da privacidade dos dados pessoais em um cenário digital cada vez mais interligado. À medida que as regulamentações de privacidade se tornam mais rigorosas e as ameaças à integridade dos dados aumentam, esse fenômeno continuará a se transformar para enfrentar os desafios emergentes. Isso proporciona uma camada suplementar de segurança ao mesmo tempo em que preserva a utilidade dos dados para análises e pesquisas legítimas.

Os dados tornados anônimos ou pseudonimizados se apresentam como uma possibilidade para o treinamento de modelos de IA com dados sensíveis sem comprometer a confidencialidade dos indivíduos. Empresas e pesquisadores podem compartilhar informações para treinar modelos de maneira colaborativa, assegurando que a identidade dos usuários originais permaneça oculta. Entretanto, o risco da reversibilidade ainda paira fortemente sobre o ar.

Considerando as possibilidades tecnológicas e legais até o momento, acreditamos que em aderência a normativas como a LGPD e a GDPR, estratégias de tornar anônimos e pseudonimizar auxiliam instituições a prevenir penalidades e a preservar a privacidade dos usuários. Isso é alcançado mediante a obtenção de consentimento adequado (dentre outras formas de tratamento), fomentando a inovação responsável e possibilitando que cientistas de dados e pesquisadores lidem com informações sensíveis para impulsionar progressos em IA, tudo isso enquanto resguardam os direitos de privacidade dos indivíduos.

A conformidade legal é outra esfera na qual a anonimização e pseudonimização assumem uma importância crucial. Regulamentações rigorosas, como as mencionadas no parágrafo anterior, estabelecem padrões rigorosos para a manipulação de dados pessoais. Embora o uso eficaz dessas técnicas seja fundamental para ajudar as organizações a cumprirem tais regulamentações, é vital abordar criticamente alguns desafios inerentes. Por exemplo, a eficácia real dessas técnicas em garantir a conformidade total e prevenir violações de dados permanece uma preocupação, especialmente diante das rápidas mudanças nas tecnologias de análise de dados.

Nesse sentido, ponderar sobre a regulação da inteligência artificial se torna uma tarefa ainda mais complexa, pois a complexidade dos modelos de IA, especialmente em ambientes colaborativos e de compartilhamento de dados, demanda uma revisão constante e adaptação das normativas existentes. O desafio reside em criar regulamentações que incentivem a inovação e o progresso tecnológico, ao mesmo tempo em que garantem a proteção efetiva dos direitos individuais e a mitigação dos riscos associados à manipulação de dados sensíveis.

A necessidade de transparência nas práticas de IA, a definição de limites claros sobre o uso de dados, a consideração de possíveis vieses nos algoritmos e a abordagem proativa para proteger a privacidade são aspectos cruciais que devem ser incorporados à regulação da inteligência artificial, conforme mencionado no ponto final do capítulo anterior. É um equilíbrio delicado entre incentivar a inovação e garantir que as tecnologias de IA sejam utilizadas de maneira ética e responsável.

Ademais, é crucial levar em conta o contexto no qual essas estratégias são empregadas. Diversos conjuntos de dados e algoritmos de inteligência artificial apresentam requisitos específicos de confidencialidade e resguardo. Logo, a efetividade das práticas de tornar anônimos e pseudonimizar pode variar consideravelmente conforme o contexto no qual são adotadas.

Portanto, a regulação da inteligência artificial enfrenta o desafio contínuo de se manter relevante e eficaz em um cenário em constante evolução, onde as técnicas de proteção de dados, como a anonimização, desempenham um papel vital na busca por um equilíbrio entre progresso tecnológico e respeito pelos direitos individuais. Além disso, é crucial envolver especialistas em segurança de dados e ética para identificar potenciais lacunas e propor melhorias no texto legal.

Embora as práticas aqui discutidas visem proteger a privacidade dos usuários, é importante reconhecer que a anonimização e pseudonimização não garantem, por si só, total segurança e invulnerabilidade contra possíveis brechas de privacidade. Além disso, a garantia de consentimento adequado, embora seja destacada como uma prática essencial, também levanta questionamentos sobre como esse consentimento é obtido e se os usuários têm compreensão suficiente sobre como seus dados serão realmente utilizados.

Em suma, enquanto a anonimização e pseudonimização são ferramentas valiosas na busca pela conformidade legal e na construção da confiança do público, é imperativo abordar criticamente suas limitações e considerar práticas complementares para garantir uma proteção robusta dos dados pessoais.

A análise da efetividade das práticas de tornar anônimos e pseudonimizar na redução dos riscos de privacidade é um percurso em constante desenvolvimento. A rápida transformação da tecnologia demanda uma abordagem propositiva e ajustável para assegurar que a confidencialidade dos indivíduos seja preservada de modo sólido e eficiente, antecipando-se às ameaças e desafios que constantemente se alteram no cenário digital contemporâneo.

3.2 REIDENTIFICAÇÃO E PRINCÍPIOS FUNDAMENTAIS DE PROTEÇÃO DE DADOS EM SISTEMAS DE IA: FINALIDADE, MINIMIZAÇÃO E PRESTAÇÃO DE CONTAS

No ponto anterior, introduzimos os conceitos trabalhados neste capítulo como anonimização e pseudoanonimização, debatemos sobre os métodos para se alcançar tais fins e iniciamos o debate relacionado à eficácia desses. Um ponto crucial neste último item é a possibilidade de reidentificação frente às novas tecnologias que utilizam processamento em massa de dados e aprendizado de máquina.

A reidentificação se manifesta quando dados, à primeira vista, não identificáveis, podem ser vinculados a informações externas para revelar a fonte original desses dados. Os progressos na inteligência artificial, especialmente no âmbito do aprendizado de máquina, possibilitaram que os algoritmos discernissem padrões intricados e delicados nos dados, abrangendo até mesmo aqueles que inicialmente foram tornados aparentemente anônimos.

A anonimização é uma técnica relativamente eficaz para preservar a privacidade, contudo, requer a implementação de critérios rigorosos e abordagens contemporâneas. Porém, não há qualquer indicação, seja por meio de legislações ou regulamentações, sobre os critérios e abordagens que precisam ser seguidos para que a anonimização seja considerada minimamente efetiva, conforme demonstrado anteriormente.[206]

Marcadores indiretos desempenham um papel central na reidentificação de dados tornados anônimos, representando uma das categorias de dados auxiliares. Apesar de um conjunto de dados ter sido minuciosamente tornado anônimo, se um algoritmo de inteligência artificial consegue associar padrões específicos nos dados tornados anônimos com informações em um conjunto de dados público, a identificação dos indivíduos relacionados torna-se factível.

Em relação à LGPD, um ponto controverso reside no fato de que o diploma dispõe em seu artigo 12 que "Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido".

Entretanto, ao definir anonimização no artigo 5º, também utiliza o termo "razoáveis", isto é, "[...] utilização de meios técnicos razoáveis e disponíveis no momento do tratamento".

---

[206] OLIVEIRA FILHO, Eduardo Luiz de. *Re-Identificação de Dados Anonimizados:* considerações de privacidade e responsabilidade na mineração de prescrições médicas. 2020. 126 f. Dissertação (Mestrado) - Curso de Mestrado Profissional em Direito, Escola de Direito de São Paulo, Fundação Getulio Vargas, São Paulo, 2020. Disponível em: https://repositorio.fgv.br/items/c1d8dcb2-0ffe-4f7e-829d-bf242b5066d7. Acessado em: 28 de outubro de 2023. p. 61.

Portanto, é possível que ao momento do tratamento os responsáveis empreguem métodos razoáveis para a anonimização e depois de um curso temporal e avanços tecnológicos esta seja revertida, passando a informação a voltar a se configurar como dado pessoal.

A situação acima traz ao debate questões relacionadas à responsabilidade dos controladores e operadores, uma vez que, conforme exposto no ponto anterior, o procedimento é sempre realizado com o objetivo de ser irreversível, mas não é possível prever como as tecnologias do futuro (próximo ou não) irão se comportar, de forma que consideramos provável o aumento da capacidade de reversão.

A LGPD estipula que o critério em questão está condicionado a elementos particulares, tais como despesas e intervalo requerido para reverter o procedimento de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios.[207] Embora a Lei faça referência aos elementos da razoabilidade, ela não especifica o custo e o período necessários. A aquisição de bancos de dados e a correlação de informações adicionais são consideradas plausíveis? Uma saída envolve contemplar tecnologias futuras, mas compreender as informações re-identificadas somente quando efetivamente aplicável.[208]

Isso destaca a importância não apenas de proteger os dados em um conjunto específico, mas também de considerar o ecossistema mais amplo de dados disponíveis publicamente. Além disso, a reidentificação é exacerbada pela prática de compartilhar dados entre diferentes organizações e plataformas, conforme mais dados são compartilhados para fins de pesquisa ou colaboração, o risco de reidentificação aumenta significativamente. Mesmo pequenas brechas nas técnicas de anonimização podem ser exploradas quando dados de diferentes fontes são combinados, tornando a proteção da privacidade um desafio monumental.

Outro fator crítico é a natureza dinâmica dos dados. O que é seguro hoje pode não ser seguro amanhã. Com a evolução constante da tecnologia de IA, novos métodos de reidentificação estão constantemente sendo desenvolvidos. Assim, as técnicas de anonimização

---

[207] Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.
§ 1º A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios.

[208] OLIVEIRA FILHO, Eduardo Luiz de. *Re-Identificação de Dados Anonimizados:* considerações de privacidade e responsabilidade na mineração de prescrições médicas. 2020. 126 f. Dissertação (Mestrado) - Curso de Mestrado Profissional em Direito, Escola de Direito de São Paulo, Fundação Getulio Vargas, São Paulo, 2020. Disponível em: https://repositorio.fgv.br/items/c1d8dcb2-0ffe-4f7e-829d-bf242b5066d7. Acessado em: 28 de outubro de 2023. p. 72-73.

devem acompanhar esse ritmo, adaptando-se continuamente para garantir que permaneçam à frente das estratégias de reidentificação.[209]

Para enfrentar esses desafios, é essencial adotar uma abordagem multifacetada. Além de melhorar as técnicas de anonimização, é crucial educar as partes envolvidas sobre os riscos da reidentificação. A conscientização é o primeiro passo para uma proteção mais eficaz.

Além disso, políticas e regulamentações rigorosas devem ser implementadas para controlar a coleta e o compartilhamento de dados. As organizações também devem investir em pesquisa contínua para desenvolver técnicas de anonimização mais avançadas e robustas, capazes de resistir aos avanços rápidos na análise de dados.

Iain Cockburn, Rebeca Henderson e Scott Stern defendem que a inteligência artificial deve ser vista como uma tecnologia de propósito geral (TGP), em razão de suas características: i) é empregada em praticamente todos os segmentos econômicos; ii) provoca mais avanços e aperfeiçoa a performance nos setores em que é utilizada; iii) amplia o potencial de pesquisa e desenvolvimento; e iv) torna-se cada vez mais essencial como instrumento primordial a novas descobertas, criações e inovações.[210]

Nesse sentido, para Glauco Arbix, a atual inteligência artificial é um conjunto de tecnologias que tem a capacidade de produzir outras tecnologias, novas técnicas e aplicações, e, por esse motivo, suas propriedades são diferentes das de outras inovações que são lançadas no mercado. O autor faz uma consideração em seu texto que consideramos bastante apropriada sobre a forma de abordar a inteligência artificial, destacada a seguir:[211]

> Como pequeno alerta, é preciso dizer que este texto não tratará a IA como um novo Frankenstein que, sem amarras, passou a assombrar seus criadores. Tampouco a IA será abordada como mais uma tecnologia, semelhante a tantas outras que ajudaram a tecer a história. Diferentemente, a IA é apresentada como uma poderosa força transformadora.

O propósito aqui é buscar parâmetros para balizar a discussão acerca do tema, não proclamar contra os avanços científicos da tecnologia em questão. Dessa forma, vislumbramos na análise dos princípios da proteção de dados em legislações de IA, um direcionamento que busca se atentar às preocupações demonstradas neste trabalho.

---

[209] PRATA, Paula *et al.* Garantia de Privacidade Versus Utilidade dos Dados em Anonimização: um estudo no ensino superior. *Revista Ibérica de Sistemas e Tecnologias de Informação,* nº 40, p. 112-127, 2020.

[210] COCKBURN, Iain M.; HENDERSON, Rebecca; STERN, Scott. The impact of artificial intelligence on innovation: An exploratory analysis. *In: The economics of artificial intelligence:* An agenda. University of Chicago Press, 2018. p. 115-146. p. 116 e 117.

[211] ARBIX, Glauco. "Algoritmos não são inteligentes nem têm ética, nós temos": a transparência no centro da construção de uma ia ética. In: COZMAN, Fábio G.; PLONSKI, Guilherme Ary; NERI, Hugo. *Inteligência artificial:* avanços e tendências. São Paulo: Instituto de Estudos Avançados, 2021. Cap. 11. p. 260-284.

Em última análise, a discussão sobre como os algoritmos de IA podem reidentificar informações pessoais após a anonimização não é apenas uma questão técnica, mas uma questão ética e social profunda. Proteger a privacidade em um mundo cada vez mais conectado e *data-driven* exige uma vigilância constante, uma compreensão aprofundada dos riscos e um compromisso inabalável com a inovação responsável.

Nikolaos M. Siafakas argumenta que a área mais bem-sucedida em relação à prática da ética em sua profissão é a medicina. Para ele, existem muitos direcionamentos éticos para programadores, mas estes estão cheios de promessas superficiais, fiscalização e erros. A partir disso, declara que um juramento de Hipócrates para cientistas de inteligência artificial poderia ter mais eficiência que diretrizes vagas.

O juramento de Hipócrates é realizado pelos estudantes de medicina ao colar grau e se tornarem efetivamente médicos. Nesta ocasião, uma das promessas é a de não fazer mal a vida humana. O autor afirma que um tal juramento poderia contribuir para a formação de um vínculo entre os cientistas e a ética, de modo geral. Além disso, outra fundamentação para sua sugestão é a de que esta daria ênfase na responsabilidade individual e priorizar o bem da humanidade em detrimento de avanços tecnológicos desenfreados.[212]

Ainda que ética na inteligência artificial não esteja dentro do escopo deste texto, o artigo em questão chamou atenção justamente pela qualidade inédita da proposta, embora não possamos concordar completamente quanto à não necessidade de princípios norteadores ou regulações que acompanhem tal lógica, o projeto relacionado ao juramento não nos parece completamente disparatado. A ideia de propagação de direitos humanos em diversos formatos ou frentes vai ao encontro de posicionamentos por nós defendidos.

Nos últimos anos, a interseção entre a inteligência artificial e a proteção de dados se tornou um campo de crescente importância e complexidade. À medida que as sociedades se tornam cada vez mais dependentes de algoritmos de IA para tomar decisões importantes, o exame dos princípios fundamentais de proteção de dados torna-se crucial para garantir a privacidade e a segurança dos indivíduos.

O princípio da finalidade, conforme a LGPD, estabelece que os dados pessoais devem ser coletados para propósitos específicos, explícitos e legítimos, e não devem ser processados de maneira incompatível com esses propósitos.[213] Quando aplicado à IA, isso significa que os

---

[212] SIAFAKAS, N. Do We Need a Hippocratic Oath for Artificial Intelligence Scientists? *AI Magazine*, volume 42, nº 4, p. 57-61, 2022. Disponível em: https://ojs.aaai.org/aimagazine/index.php/aimagazine/article/view/15090. Acessado em: 11 de abril de 2023. p. 57-59.

[213] Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

desenvolvedores e operadores de algoritmos devem ter um propósito claro e justificável para coletar e processar dados pessoais.

Um sistema de IA usado para análise de padrões de consumo deve coletar apenas os dados necessários para essa finalidade específica, evitando a coleta excessiva e não relacionada ao propósito original. Além disso, a transparência sobre esses propósitos torna-se essencial, permitindo que os usuários entendam como suas informações serão utilizadas.

O princípio da minimização (também chamado de princípio da necessidade) de dados estabelece que apenas os dados estritamente necessários para atingir a finalidade especificada devem ser coletados e processados.[214] No contexto da IA, isso implica que os algoritmos devem ser projetados para operar com a menor quantidade de dados possível, reduzindo assim o risco associado ao processamento excessivo de informações pessoais.

Estratégias como a anonimização e a pseudonimização, discutidas anteriormente, são essenciais para garantir que os dados sejam reduzidos ao mínimo necessário para que os algoritmos funcionem eficazmente, enquanto ainda preservam a privacidade.

O princípio da prestação de contas refere-se à responsabilidade dos controladores de dados (organizações ou indivíduos que determinam os propósitos e meios de processamento de dados) em garantir a conformidade com os princípios de proteção de dados.[215] Para algoritmos de IA, isso significa que as organizações são responsáveis por garantir que seus sistemas operem de maneira ética e estejam em conformidade com as leis de proteção de dados.

À medida que os algoritmos de IA continuam a moldar nosso mundo, a adoção responsável desses princípios não apenas protege a privacidade dos dados, mas também fortalece a confiança dos usuários na tecnologia e naqueles que a desenvolvem e operam. Projetar sistemas de inteligência artificial que respeitem os princípios fundamentais de proteção de dados, como finalidade, minimização de dados e prestação de contas, exige uma abordagem multidisciplinar que combina conhecimentos em ciência da computação, ética, legislação e segurança de dados.

De maneira similar ao emprego de técnicas de aprendizagem de máquina, pode-se utilizar para facilitar a aplicação prática de sistemas fundamentados em conhecimento, as

---

I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

[214] Art. 6º, III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados/ Lei nº 13.709/2018 (LGPD).

[215] Art. 6º, X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas/Lei nº 13.709/2018 (LGPD).

representações do campo que esses fornecem podem ser valiosas para elucidar como a inteligência artificial no âmbito jurídico alcança suas conclusões. No contexto do Direito, a compreensibilidade da IA é especialmente crucial, pois qualquer ato ou decisão judicial ou administrativa só é legalmente aceitável na medida em que possa ser devidamente justificado.

Neste cenário, tanto o processo quanto o conteúdo da justificação são tão significativos quanto o resultado. A exigência de esclarecimento não é apenas uma condição para que os sistemas inteligentes possam ser empregados em contextos legais, mas também é uma exigência para que as previsões da inteligência artificial sejam efetivas.[216]

Ao comparar o emprego de técnicas de aprendizagem de máquina com a necessidade de compreensão das representações do campo jurídico, ressalta-se a relevância de uma abordagem que não apenas produza resultados, mas também permita entender como esses resultados são alcançados. Isso é crucial no Direito, onde a legitimidade de atos e decisões está intimamente ligada à capacidade de justificação. A ênfase na compreensibilidade da IA destaca a importância não apenas de gerar previsões precisas, mas também de comunicá-las de maneira transparente e acessível.

Assim, a inclusão de abordagens computacionais para o processamento da argumentação jurídica, juntamente com as técnicas já estabelecidas para o processamento de linguagem jurídica, possibilitará aos sistemas reconhecerem os argumentos presentes em documentos legais e, com base nisso, anteciparem o desfecho de forma mais precisa e compreensível para os observadores humanos.

O caminho para integrar os modelos de previsão envolve, por um lado, o avanço de programas capazes de identificar elementos pertinentes ou argumentos em documentos legais, a fim de gerar premissas para sistemas computacionais que adotem lógicas jurídicas e de argumentação. Por outro lado, requer o desenvolvimento e aprimoramento dos sistemas de argumentação e elaboração de justificativas, baseados em elementos e argumentos, para que consigam processar argumentos e elementos extraídos automaticamente (por meio de aprendizado de máquina) de textos e documentos jurídicos.

Com isso, é viável criar modelos de argumentação que possam, a partir de textos jurídicos com pouca ou nenhuma intervenção especial, não apenas oferecer previsões empíricas derivadas de correlações estatísticas, mas também previsões normativas baseadas na força

[216] MARANHÃO, Juliano Souza de Albuquerque; FLORÊNCIO, Juliana Abrusio; ALMADA, Marco. Inteligência artificial aplicada ao direito e o direito da inteligência artificial. *Suprema:* revista de estudos constitucionais, 2021, v. 1, n. 1, p. 154-180. Disponível em: https://hdl.handle.net/1814/71840. Acesso em: 07 mar. 2024.

argumentativa do caso em relação aos precedentes, além da construção de justificativas legais a partir de argumentos compreensíveis.[217]

Ao combinar técnicas já estabelecidas de processamento de linguagem jurídica com avanços na identificação de elementos relevantes, os sistemas podem antecipar resultados de forma mais precisa e compreensível para os observadores humanos. Essa abordagem não só visa processar argumentos e elementos extraídos automaticamente de documentos jurídicos, mas também busca criar modelos de argumentação capazes de oferecer previsões normativas e justificativas legais a partir de argumentos compreensíveis.

Isso reflete a importância não apenas de produzir previsões baseadas em correlações estatísticas, mas também de considerar a força argumentativa dos casos em relação aos precedentes legais, garantindo assim uma abordagem mais holística e eficaz na aplicação da inteligência artificial no campo jurídico.

A Organização para Cooperação e Desenvolvimento Econômico (OCDE), conforme definição própria, é uma organização que trabalha para construir melhores políticas para vidas melhores. Juntos com governos, políticos e cidadãos, trabalham para estabelecer padrões internacionais baseados em evidências e encontrar soluções para uma gama de questões sociais, econômicas e ambientais.[218]

As decisões da OECD (Organization for Economic Cooperation and Development) são vinculantes apenas aos seus países membros e apesar de não se nivelar a um tratado internacional, demandam obrigatoriedade. Com relação aos demais países, ainda que não sejam membro, acabam sendo afetados pelas resoluções indiretamente. O Brasil não é parte da organização, entretanto, é identificado como parceiro-chave desde 1994.[219]

Em 2019, o Comitê de Políticas Públicas para Economia Digital publicou um documento denominado "*Recomendation of the Council on OECD Legal Instruments Artificial Intelligence*",[220] a organização também publica declarações com esta natureza de recomendações, dessa forma, os países membro não estão vinculados a elas.

A finalidade principal do referido documento é fomentar o progresso e a credibilidade no que diz respeito à inteligência artificial, por meio do estímulo à administração consciente e

---

[217] MARANHÃO, Juliano Souza de Albuquerque; FLORÊNCIO, Juliana Abrusio; ALMADA, Marco. Inteligência artificial aplicada ao direito e o direito da inteligência artificial. *Suprema:* revista de estudos constitucionais, 2021, v. 1, n. 1, p. 154-180. Disponível em: https://hdl.handle.net/1814/71840. Acesso em: 07 mar. 2024.
[218] OECD. *About us.* Disponível em: https://www.oecd.org/about/. Acessado em 14 de abril de 2023.
[219] OECD. *A OCDE e o Brasil:* Uma relação mutuamente benéfica. Disponível em: https://www.oecd.org/latin-america/paises/brasil-portugues/. Acesso em: 14 abr. 2023.
[220] OECD. *Recomendation of the Council on OECD Legal Instruments Artificial Intelligence. Committe on Digital Economy Policy.* 2019. Disponível em: https://legalinstruments.oecd.org/api/print?ids=648&lan=en. Acesso em: 14 abr. 2023.

responsável desta, observando os princípios democráticos e assegurando o os direitos fundamentais.

Quanto ao teor dos princípios, são eles: 1) Crescimento inclusivo; 2) Desenvolvimento sustentável e bem-estar; 3) Valores centrados no ser humano e equidade; 4) Transparência e explicabilidade; 5) Robustez; 6) Segurança; e 7) Responsabilidade.

Entre o final de 2019 e início de 2020, o Brasil, por meio do Ministério da Ciência, Tecnologia, Inovações e Comunicações, realizou uma Consulta Pública para obter sugestões voltadas a estabelecer a próxima Estratégia Nacional de Inteligência Artificial, utilizando esses Princípios como base.[221]

No entanto, além de atuarem como pontos de orientação política para o Legislador, podemos abordar a questão do impacto potencial e presente desses Princípios em relação à proteção de dados. Inicialmente podemos pontuar que estes são compatíveis aos enunciados pela LGPD, em seu artigo 2º. Entretanto, é necessário observar com mais cautela o disposto no artigo 6º.

Para Manuel Masseno, o conteúdo de cada um desses postulados também pode ser completado pelos Princípios da OCDE, por meio de interpretação e sem quaisquer atritos valorativos, aprofundando-os. Além disso, de maneira semelhante, uma operação desse tipo pode ser efetuada também no que diz respeito às normas cuja implementação requer uma consideração especial da IA. Primeiramente, e de forma mais clara, isso se aplica ao regime dos "processamentos automatizados" (Artigo 20).[222]

O autor complementa sua avaliação para tratar dos pontos controvertidos, isso se verifica com a dispensa da "[...] revisão de decisões tomadas exclusivamente com base em processamento automatizado de dados pessoais que impactem seus interesses [pelo] titular dos dados" ser realizada "por pessoa natural" (Artigo 20 "*caput*"), assim como no segundo Princípio da OCDE, que estipula a "[...] possibilidade de intervenção humana, quando necessário".

Resumidamente, uma considerável parcela dos Governos Globais adere aos Princípios da OCDE ou a textos com significados similares, no que tange à importância de as decisões finais serem tomadas por seres humanos, especialmente quando afetam os Direitos das pessoas naturais.[223]

---

[221] PARTICIPA. *Estratégia brasileira de inteligência artificial.* 2020. Disponível em: http://participa.br/profile/estrategia-brasileira-de-inteligencia-artificial. Acesso em: 14 abr. 2023.

[222] MASSENO, Manuel David. Das Consequências Jurídicas da Adesão do Brasil aos Princípios da OCDE Para a Inteligência Artificial, Especialmente Em Matéria De Proteção de Dados. *Campo Jurídico*, v. 8, n. 2, p. 113-122, 1 jul. 2020. Centro Universitário São Francisco de Barreiras. Disponível em: http://dx.doi.org/10.37497/revcampojur.v8i2.659. Acesso em: 26 nov. 2023.

[223] *Ibidem*.

Dessa forma, até que a Lei Geral de Proteção de Dados seja modificada de forma a se alinhar aos Princípios, cabe ao Supremo Tribunal Federal extrair as devidas consequências do fato de que "a dignidade da pessoa humana" é um dos "fundamentos" da "República Federativa do Brasil" (Artigo 1º III da Constituição Federal de 1988). Em outras palavras, compreender que a única interpretação constitucionalmente válida requer a revisão das decisões automatizadas por uma pessoa natural.[224]

Considerando a relação acima abordada podemos observar a conexão com alguns dos princípios fundamentais da LGPD: minimização e prestação de contas, quanto à minimização, o texto destaca a importância da administração consciente e responsável da inteligência artificial, observando princípios democráticos e garantindo os direitos fundamentais. Essa abordagem está em sintonia com o princípio de minimização da LGPD, que preconiza que o tratamento de dados deve ser limitado ao mínimo necessário para a realização de suas finalidades.

No que diz respeito à prestação de contas, o texto menciona a necessidade de uma revisão das decisões automatizadas por uma pessoa natural, destacando a importância da intervenção humana quando necessário. Esse aspecto pode ser relacionado ao princípio de prestação de contas da LGPD, que exige que o controlador seja capaz de demonstrar a adoção de medidas eficazes para garantir a conformidade com a lei.

Assim, podemos inferir que a abordagem da OCDE em relação à inteligência artificial, conforme descrito no texto, converge com alguns dos princípios essenciais da LGPD, fortalecendo a ideia de uma regulamentação alinhada internacionalmente e reforçando a necessidade de considerar princípios na implementação de tecnologias como a inteligência artificial.

Os princípios de proteção de dados devem ser incorporados desde a concepção do sistema de IA. Isso implica considerar a privacidade como um aspecto fundamental do *design*, garantindo que apenas os dados estritamente necessários para a finalidade específica sejam coletados e processados. Um *design* por padrão para a privacidade significa que os usuários não precisam tomar medidas extras para proteger suas informações; a proteção de dados é incorporada automaticamente nos sistemas.[225]

---

[224] *Ibidem*.

[225] BARTH, Susanne; IONITA, Dan; HARTEL, Pieter. Understanding online privacy—a systematic review of privacy visualizations and privacy by design guidelines. *ACM Computing Surveys (CSUR)*, v. 55, n. 3, p. 1-37, 2022. Disponível em: https://doi.org/10.1145/3502288. Acesso em: 30 nov. 2023.

Os sistemas de IA devem ser transparentes e interpretáveis, permitindo que os usuários entendam como seus dados estão sendo usados. Métodos avançados de IA, como Redes Neurais Profundas, muitas vezes são considerados caixas-pretas, dificultando a compreensão do processo de tomada de decisão, conforme mencionado ao final do capítulo anterior.

Estabelecer uma estrutura de governança clara e responsável é crucial. Designar um encarregado de proteção de dados (DPO) ou um comitê de ética para supervisionar a conformidade com os princípios de proteção de dados é uma prática recomendada. No entanto, é fundamental adotar uma perspectiva crítica ao implementar essas medidas.

A nomeação de um DPO ou comitê de ética é um passo positivo, mas é preciso questionar se esses órgãos têm poderes efetivos e autonomia para agir em prol da proteção de dados ou se são apenas figurações formais. Além disso, a eficácia desses mecanismos depende da capacidade de adaptar-se às mudanças rápidas na tecnologia e nas práticas de manipulação de dados.

Da mesma forma, realizar avaliações de impacto à privacidade é considerado fundamental para identificar e mitigar riscos. No entanto, é importante questionar se essas avaliações são realizadas de maneira abrangente e se são incorporadas proativamente no desenvolvimento do sistema de IA. A crítica construtiva nesse contexto envolve avaliar se as avaliações de impacto são uma formalidade superficial ou uma prática genuína e efetiva para garantir a proteção da privacidade.

Enquanto a estrutura de governança proposta é um passo positivo, a reflexão crítica é vital para garantir que essas práticas não se tornem meros exercícios burocráticos, mas sim contribuam efetivamente para a proteção da privacidade ao longo da evolução da inteligência artificial.

Nesse sentido, a proteção de dados *by design* no ordenamento jurídico brasileiro está delineada em determinados artigos da LGPD, como, por exemplo o 46. Em sua introdução, este dispositivo estabelece que os responsáveis pelo tratamento de informações pessoais devem implementar medidas de segurança, tanto técnicas quanto administrativas, para resguardar os dados pessoais. Em contraste com o que é estipulado no regulamento europeu similar que não especificou tais medidas com base nos riscos associados ao tratamento de dados pessoais.

Em vez disso, exige que as medidas adotadas sejam competentes para proteger os dados pessoais contra os fatores indicados no dispositivo. Entretanto, a necessidade de implementar medidas que evitem riscos provenientes da proteção de dados decorre do fato de que a prevenção constitui um princípio geral do sistema brasileiro de proteção de dados Artigo

6, VIII da LGPD.[226] A competência mencionada no início do Artigo 46 da LGPD, portanto, deve ser analisada considerando a eficácia de um conjunto de medidas em evitar — ou pelo menos mitigar — os riscos resultantes do tratamento de dados pessoais.[227]

Essenciais salvaguardas ao titular de dados podem adotar uma variedade de formas. Embora a especificação dessas salvaguardas não esteja explicitamente estabelecida no texto da LGPD, é viável delimitá-la através da interpretação dos termos e das contribuições das experiências internacionais. Medidas técnicas referem-se à implementação de tecnologias que diminuam ou erradiquem os perigos associados ao processamento, como a anonimização dos dados a serem manipulados.

Por outro lado, medidas administrativas, também chamadas de organizacionais, dizem respeito ao contexto institucional no qual um sistema é empregado. Por fim, as medidas de segurança compreendem tanto medidas técnicas quanto administrativas, destacadas pelo legislador devido à sua finalidade: a prevenção de acessos não autorizados e a salvaguarda contra a destruição, perda, alteração, comunicação ou disseminação dos dados Artigo 6º, VII/LGPD.[228][229]

Os autores discutem a importância de adotar uma abordagem combinada de medidas técnicas e administrativas para garantir a proteção eficaz dos dados pessoais, conforme defendido ao longo desta exposição; com destaque para a necessidade de adaptar essas medidas de acordo com o contexto específico de tratamento de dados, reconhecendo que diferentes problemas podem demandar soluções distintas.

Além disso, o texto enfatiza a importância de avaliar continuamente o contexto operacional e ajustar as práticas de proteção de dados conforme necessário. Isso reflete a natureza dinâmica do tratamento de dados e a necessidade de adaptação constante para garantir a proteção dos direitos dos titulares de dados. Em suma destaca-se a complexidade e a importância de uma abordagem holística e flexível para a proteção de dados pessoais, levando

---

[226] Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

[227] LASMAR ALMADA, M. A.; SOUZA DE ALBUQUERQUE MARANHÃO, J. Contribuições e Limites da Lei Geral de Proteção de Dados para a Regulação da Inteligência Artificial no Brasil. *Direito Público*, [S. l.], v. 20, n. 106, 2023. DOI: 10.11117/rdp.v20i106.6957. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/6957. Acesso em: 13 mar. 2024.

[228] VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

[229] LASMAR ALMADA, M. A.; SOUZA DE ALBUQUERQUE MARANHÃO, J. Contribuições e Limites da Lei Geral de Proteção de Dados para a Regulação da Inteligência Artificial no Brasil. *Direito Público*, [S. l.], v. 20, n. 106, 2023. DOI: 10.11117/rdp.v20i106.6957. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/6957. Acesso em: 13 mar. 2024.

em consideração tanto as necessidades específicas do contexto quanto as melhores práticas disponíveis.

A preservação eficaz da privacidade demanda uma abordagem polivalente. Além de aprimorar métodos de tornar anônimo, é crucial instruir todas as partes envolvidas acerca dos perigos da reidentificação. Diretrizes rigorosas devem ser aplicadas para supervisionar a aquisição e a partilha de dados, e as organizações devem dedicar recursos à pesquisa incessante para formular técnicas de tornar anônimo mais avançadas.

Em última análise, a proteção da privacidade dos usuários transcende a mera obrigação legal; representa igualmente uma responsabilidade ética e social. Nesse contexto, adotar uma abordagem proativa e multidisciplinar é essencial para a construção de sistemas de inteligência artificial (IA) que sejam inovadores, éticos e confiáveis.

A dimensão social dessa responsabilidade destaca o impacto mais amplo que a IA pode ter na sociedade. A consideração ética e social não se limita apenas à proteção individual da privacidade, mas também envolve avaliar como a implementação da IA pode influenciar comunidades e grupos sociais de maneira mais ampla.

3.3 DESAFIOS REGULATÓRIOS NA INTEGRAÇÃO DE IA: ANÁLISE CRÍTICA DOS MARCOS LEGAIS DE PROTEÇÃO DE DADOS (GDPR E LGPD)

No ponto anterior, iniciamos a abordagem acerca dos desafios da aplicação das legislações de proteção de dados no contexto da IA, agora passaremos a uma análise comparativa entre os marcos regulatórios referentes a este assunto, se poderiam se adequar a uma eventual regulação da inteligência artificial.

No Brasil, existem alguns projetos de lei sobre uma regulamentação da inteligência artificial sendo debatidos, entretanto, o principal texto é o elaborado pela Comissão de Juristas responsável por subsidiar elaboração de substitutivo sobre inteligência artificial no Brasil. Este conta com uma ampla lista de princípios.

Em sua contribuição para a comissão, André Gualtieri criticou a ausência de um princípio relativo à autonomia. Para o autor, tal ausência implicaria em ceder às máquinas um poder de decisão que antes era exclusivo dos seres humanos. Afirma, ainda, que o risco da não inclusão é a diminuição da autonomia humana.[230]

---

[230] GUALTIERI, André. *Contribuição à Comissão de Juristas do Senado Federal sobre Inteligência Artificial.* Senado Federal, 2022. Disponível em: https://legis.senado.leg.br/comissoes/arquivos?ap=6916&codcol=2504. Acesso em: 13 abr. 2023. p. 6.

Também em contribuição para a comissão, o Grupo de Pesquisa de Direito e Inovação da Universidade Presbiteriana Mackenzie[231] aponta que a regulação em questão poderia ocorrer de duas maneiras. A primeira com inspiração no modelo europeu, com documentos mais específicos (Diretivas, Recomendações e Resoluções) sobre os assuntos: aspectos éticos, propriedade intelectual, responsabilidade civil, direito penal, educação, cultura e audiovisual, dentre outros.

A segunda, através de microssistemas normativos de base principiológica com abordagem de aspectos civis, penais e administrativos, abordando diversos setores em uma mesma Lei, como ocorre, por exemplo, no Código de Defesa do Consumidor, que admite complementação de outros instrumentos mais específicos. Embora ambos os modelos sejam razoáveis, o grupo acredita que o segundo seria mais adaptável à realidade brasileira.

O grupo alerta para a necessidade da observância da lógica sistemática, isto é, a regulamentação não pode ser pensada visando apenas a criação de novas regras, mas sim buscando estabelecer diálogo com aquelas que já existem no ordenamento e permeiam o tema, para evitar contradições e sobreposições desnecessárias. Para eles, o projeto não abarca nenhum dos modelos mencionados como possíveis, carece de instrumentos de efetivação e definições sobre quais órgãos teriam o poder de polícia.

Dessa forma, foram elaboradas quatro recomendações, dispostas a seguir:

> a) A revisão do modelo de regulamentação previsto no PL 21/2020 para incorporar ou o modelo da Comunidade Europeia, de documentos mais específicos, ou um segundo, de microssistema normativo com base principiológica, a exemplo do Código de Defesa do Consumidor; b) Definição expressa sobre a criação de nova Agência Reguladora, com poder de polícia e de editar normas infralegais ou aproveitamento de estruturas administrativas e regulações já existentes (ANPD, ANS, ANATEL, entre outras); c) Aproveitamento das conquistas sociais trazidas pelo CDC, Marco Civil da Internet e LGPD na regulamentação do Marco Legal da IA; e e) Definições de responsabilidades específicas de prestações de contas e transparência conforme o porte da empresa, considerando os fatores: volume de dados processados; dados sensíveis e intensidade dos riscos.[232]

Nesse sentido, destacamos que a ênfase na observância da lógica sistemática na regulamentação é crucial, evitando contradições e sobreposições desnecessárias com as leis existentes. As recomendações elaboradas, como a revisão do modelo de regulamentação, o

---

[231] RÖHE, Anderson *et al. Contribuição à Consulta Pública sobre o Marco Regulatório da Inteligência Artificial.* Grupo de Pesquisa de Direito e Inovação (GEDI). Senado Federal, 2022. Disponível em: https://legis.senado.leg.br/comissoes/arquivos?ap=6916&codcol=2504. Acesso em: 13 abr. 2023. p. 2-3.

[232] RÖHE, Anderson *et al. Contribuição à Consulta Pública sobre o Marco Regulatório da Inteligência Artificial.* Grupo de Pesquisa de Direito e Inovação (GEDI). Senado Federal, 2022. Disponível em: https://legis.senado.leg.br/comissoes/arquivos?ap=6916&codcol=2504. Acesso em: 13 abr. 2023.

aproveitamento de estruturas administrativas existentes e a incorporação de conquistas sociais de legislações anteriores mostram-se fundamentais para um arcabouço legal robusto e eficaz.

Em outubro de 2023, a ANPD divulgou sua segunda nota técnica (Nota Técnica nº 16/2023/CGTP/ANPD) comentando o Projeto de Lei nº 2338/2023. O texto apresenta sugestões concretas de modificação ao projeto de lei, sugere um novo formato institucional, lista sete áreas de convergência relevantes entre o PL e a LGPD, além de realizar uma comparação com as práticas regulatórias de autoridades internacionais.

A análise propõe o estabelecimento de um modelo institucional para regular os sistemas de IA, composto por quatro instâncias complementares, com a Autoridade Nacional desempenhando um papel central nessa área. O modelo recomendado pela ANPD inclui uma cooperação coordenada entre entidades do Poder Executivo, órgãos reguladores setoriais, e a criação de um Conselho Consultivo, similar ao CNPD (Conselho Nacional de Proteção de Dados), para tratar especificamente da regulamentação do uso de inteligência artificial no país.

De acordo com o documento, experiências internacionais demonstram que uma abordagem centralizada, liderada por uma única autoridade, traz vantagens evidentes na formulação de normas, como observado na União Europeia, França, Holanda, entre outros países.

O texto também ressalta a proposta de transferir ao Poder Executivo, em vez da autoridade competente conforme previsto no texto atual do projeto de lei, a responsabilidade de elaborar, gerenciar, atualizar e implementar a Estratégia Brasileira de Inteligência Artificial (EBIA). De acordo com a nota técnica, caberá à ANPD, dentro de suas atribuições, contribuir para o processo de elaboração e implementação da EBIA.[233]

A influência da GDPR em várias legislações nacionais sobre informações pessoais é clara devido ao seu pioneirismo no tema. Até agora, ela permanece como o principal referencial regulatório, abrangendo de maneira ampla tanto aspectos legais quanto estruturais relacionados às questões de privacidade *online*.

Para iniciarmos, é fundamental compreender como a norma define dados pessoais, os quais, conforme o Artigo 4°, são caracterizados como "[...] qualquer informação relacionada a um indivíduo identificado ou identificável (titular dos dados)".[234] Por informação, entende-se

---

[233] BRASIL. CGTP. *ANPD*. Nota Técnica nº 16/2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/Nota_Tecnica_16ANPDIA.pdf. Acesso em: 6 mar. 2024.

[234] Para efeitos do presente regulamento, entende-se por:
1) «Dados pessoais», informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética,

estritamente qualquer dado capaz de identificar de maneira inequívoca um sujeito, seja de forma direta ou indireta, sendo esses dados passíveis de serem físicos ou virtuais. Essa abordagem ampla e progressista visa dinamizar a legislação, evitando sua obsolescência ou defasagem diante das constantes mudanças e evoluções no ambiente virtual.

Como mencionado inicialmente, o aspecto territorial do regulamento em questão abrange o manejo de informações de pessoas vinculadas à União Europeia ou dados situados na UE. Isso implica que, não importando a procedência do responsável pelo controle ou processamento (seja este de natureza pública ou privada), ao conduzir operações ou oferecer serviços nas condições mencionadas, é obrigatório aderir às diretrizes da GDPR.

Ao acessar o texto da GDPR os primeiros componentes visualizados são os chamados *recitals*, diretrizes para melhor interpretação da regulação. A transparência é abordada no nº 58, que dispõe[235]:

> O princípio da transparência exige que qualquer informação dirigida ao público ou ao titular dos dados seja concisa, facilmente acessível e de fácil compreensão, e que seja usada uma linguagem clara e simples e, além disso, quando apropriado, uma visualização. Essas informações podem ser fornecidas em formato eletrônico, por exemplo, quando dirigidas ao público, por meio de um site. Isso é particularmente relevante em situações em que a proliferação de agentes e a complexidade tecnológica da prática tornam difícil para o titular dos dados saber e entender se, por quem e com que finalidade os dados pessoais relacionados a ele estão sendo coletados, como no caso da publicidade on-line. Considerando que as crianças merecem proteção específica, qualquer informação e comunicação, quando o processamento for dirigido a uma criança, deve ser feita em uma linguagem clara e simples que a criança possa entender facilmente. (Traduzido pela autora).

A norma enfatiza o valor do princípio da transparência na comunicação de informações relacionadas à proteção de dados pessoais. Destaca que essas informações devem ser

---

mental, económica, cultural ou social dessa pessoa singular. UNIÃO EUROPEIA. Regulamento (Ue) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, Relativo À Proteção das Pessoas Singulares no Que Diz Respeito Ao Tratamento de Dados Pessoais e À Livre Circulação Desses Dados e Que Revoga A Diretiva 95/46/Ce (Regulamento Geral Sobre A Proteção de Dados) nº 679, de 27 de abril de 2016. *Jornal Oficial da União Europeia*. Estrasburgo, 04 mai. 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016R0679&qid=1701988584822. Acesso em: 27 nov. 2023.

[235] UNIÃO EUROPEIA. Regulamento (Ue) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, Relativo À Proteção das Pessoas Singulares no Que Diz Respeito Ao Tratamento de Dados Pessoais e À Livre Circulação Desses Dados e Que Revoga A Diretiva 95/46/Ce (Regulamento Geral Sobre A Proteção de Dados) nº 679, de 27 de abril de 2016. *Jornal Oficial da União Europeia*. Estrasburgo, 04 mai. 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016R0679&qid=1701988584822. Acesso em: 27 nov. 2023.

"The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used. Such information could be provided in electronic form, for example, when addressed to the public, through a website. This is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising. Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand".

apresentadas de forma clara, acessível e compreensível para o público em geral e para os próprios titulares dos dados. Além disso, sublinha a relevância especial desse princípio em contextos onde a complexidade tecnológica e a proliferação de atores tornam difícil para os titulares dos dados saber quem está coletando seus dados e com que propósito, como é o caso da publicidade online.

Outro ponto em destaque diz respeito à necessidade de que os encarregados pelo manuseio de informações notifiquem os titulares e autoridades competentes dentro de um prazo de 72 horas, caso ocorra uma divulgação não autorizada de seus dados. O descumprimento dessa obrigação pode resultar em penalidades monetárias.[236]

Um dos meios de aplicação para assegurar que esses direitos sejam exercidos, e, por conseguinte, que as obrigações sejam cumpridas pela contraparte, é a viabilidade da instituição de um cargo — tanto em organizações privadas quanto em entidades públicas — denominado *Data Protection Office*r (DPO, Diretor de Proteção de Dados, em português). O DPO é encarregado de supervisionar as atividades relacionadas a dados pessoais e garantir que todas estejam em permanente conformidade com a regulamentação. Se necessário, ele pode ser convocado para prestar esclarecimentos às autoridades reguladoras e/ou ao público.

Além da designação de um DPO, a legislação europeia atribuiu a função mais relevante no que tange à execução da lei — aconselhar, supervisionar e aplicar penalidades quando necessário — às Autoridades de Proteção de Dados (DPA, em português) específicas de cada Estado membro. Dessa forma, cada país membro da UE é encarregado de escolher o conselho que constituirá a autoridade reguladora e de determinar os poderes concedidos a ela, ou seja, as responsabilidades específicas de cada DPA estão sujeitas às leis nacionais de cada país-membro.[237]

O contexto apresentado tem relevância direta para a regulação da inteligência artificial devido à crescente interseção entre o manuseio de dados e o desenvolvimento e implementação de sistemas de IA. A definição abrangente de dados pessoais, ressalta a importância de garantir a proteção dos indivíduos em um contexto digital. Essa definição tem implicações diretas para a IA, pelas intersecções já debatidas sobre estes conceitos. Portanto, a regulamentação da IA

---

[236] Artigo 33 - Notificação de uma violação de dados pessoais à autoridade de controlo
1. Em caso de violação de dados pessoais, o responsável pelo tratamento notifica desse facto a autoridade de controlo competente nos termos do artigo 55.o, sem demora injustificada e, sempre que possível, até 72 horas após ter tido conhecimento dela, a menos que a violação dos dados pessoais não seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares. Se a notificação à autoridade de controlo não for transmitida no prazo de 72 horas, é acompanhada dos motivos do atraso.

[237] SUN, Chen *et al.* GDPRxiv: Establishing the State of the Art in GDPR Enforcement. *Proceedings on Privacy Enhancing Technologies*, v. 4, p. 484-499, 2023.

pode considerar essa definição ampla e progressista para proteger os direitos e privacidade dos indivíduos.

O aspecto territorial da GDPR, destaca a necessidade de considerar o alcance global das regulamentações sobre IA. À medida que as tecnologias de IA ultrapassam fronteiras, é crucial estabelecer padrões internacionais para garantir a consistência na proteção dos direitos dos indivíduos em contextos globais. A ênfase na notificação obrigatória de violações de dados e as penalidades associadas ao não cumprimento dessas obrigações também são princípios que podem ser aplicados à regulação da IA. A rápida notificação de incidentes é crucial para mitigar danos, e a imposição de penalidades visa garantir a conformidade e responsabilidade na utilização dessas tecnologias.

A criação do cargo de *Data Protection Officer* (DPO), mencionado no texto, é uma abordagem interessante que poderia ser adaptada para a regulamentação da IA. Ter um profissional dedicado a supervisionar as atividades relacionadas a dados pessoais em organizações que desenvolvem e implementam sistemas de IA pode fortalecer a conformidade com as regulamentações e garantir a proteção adequada dos direitos dos indivíduos. Desde que, conforme mencionado neste capítulo, este profissional tenha poderes não apenas formais.

A relevância atingida pela Lei Geral de Proteção de Dados (LGPD) alcançou uma significância inédita, especialmente diante do uso da tecnologia e da abrangente digitalização, afetando distintos setores da vida contemporânea. O início da vigência da LGPD marca um ponto crucial no sistema jurídico nacional, pois assegura segurança jurídica e uniformidade, harmonizando as normas relacionadas à proteção de dados, considerando tanto entidades públicas quanto privadas como controladoras. Sua legislação regula o manuseio de dados pessoais por qualquer entidade física ou jurídica, seja de direito privado ou público, englobando agentes privados e a Administração Pública direta e indireta. Seus propósitos visam principalmente reconhecer e proporcionar maior autonomia e controle aos indivíduos em relação às suas informações pessoais.

Entre as informações regulamentadas pela LGPD, incluem-se os dados pessoais, os dados sensíveis, os dados anonimizados e os dados pseudoanonimizados. A legislação brasileira também adota um conceito amplo de dado pessoal (artigo 5º, inciso I). Em relação à comunicação de incidente de segurança, apesar de prever o dever de reportar, o legislador brasileiro não estipulou um prazo concreto como prevê o documento europeu. A LGPD requer o seja feito em "prazo razoável".[238]

[238] Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

Sobre o encarregado de dados, "[...] aponta-se a necessidade de indicação de pessoa natural, responsável pela comunicação de qualquer informação ou fato relevante em relação ao tratamento de dados". A GDPR, no entanto, "[...] aponta que o controlador deve ter uma pessoa responsável por tudo que seja relacionado à proteção de dados".[239]

Por fim, em ambas há a previsão de sanções que variam desde advertências a proibição das atividades relacionadas ao tratamento de dados. A única diferença se dá na variação dos valores – podendo no Brasil ser simples ou diárias e com valor até 2% do faturamento da organização, limitadas a R$ 50 milhões por infração[240] e na Europa[241] podem chegar a 20 milhões de euros ou 4% do faturamento.[242]

A LGPD impulsionou a inovação econômica e tecnológica ao estabelecer regras transparentes para o uso adequado de dados pessoais no Brasil. A legislação fortaleceu a proteção da privacidade, estreitando o vínculo entre as empresas e os cidadãos, garantindo que suas informações sejam utilizadas conforme previsto na Constituição. Ela introduziu novos conceitos jurídicos e estabeleceu condições para o tratamento de informações pessoais, com penalidades para o descumprimento.

A LGPD exige mudanças significativas nos procedimentos das empresas que lidam com dados pessoais, promovendo uma maior conscientização dos consumidores sobre o valor de seus dados. Aplica-se a todos que tratam dados em território nacional, incluindo empresas estrangeiras que operam no Brasil.[243]

---

§ 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional [...].

[239] Art. 5º Para os fins desta Lei, considera-se:
VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);
PINHEIRO, Patricia Peck. *Proteção de dados pessoais:* Comentários à lei n. 13.709/2018-lgpd. Saraiva Educação SA, 2020. p. 59.

[240] Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:
II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
III - multa diária, observado o limite total a que se refere o inciso II;

[241] Artigo 83. Condições gerais para a aplicação de coimas:
1. Cada autoridade de controlo assegura que a aplicação de coimas nos termos do presente artigo relativamente a violações do presente regulamento a que se referem os n. 4, 5 e 6 é, em cada caso individual, efetiva, proporcionada e dissuasiva.
5. A violação das disposições a seguir enumeradas está sujeita, em conformidade com o n.o 2, a coimas até 20 000 000 EUR ou, no caso de uma empresa, até 4 % do seu volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior, consoante o montante que for mais elevado.

[242] PINHEIRO, Patricia Peck. *Proteção de dados pessoais:* Comentários à lei n. 13.709/2018-lgpd. Saraiva Educação SA, 2020. P. 61.

[243] FERNANDES, M. E.; NUZZI, A. P. E. Grounds of the General Data Protection Law (LGPD): A narrative review. *Research, Society and Development*, v. 11, n. 12, p. e310111234247, 2022. DOI: 10.33448/rsd-v11i12.34247. Disponível em: https://rsdjournal.org/index.php/rsd/article/view/34247. Acesso em: 7 nov. 2023.

Isto é, abrange todas as pessoas (físicas ou jurídicas) e atividades conduzidas no Brasil que guardam relação com o manuseio de dados pessoais, como a aquisição, a produção, a categorização, a utilização, o acesso, a reprodução, a transmissão, a distribuição, o processamento, o arquivamento, o armazenamento, a eliminação, a avaliação ou o controle da informação, a alteração, a transferência, a disseminação ou a extração de dados.

Assim, mesmo se a empresa ou entidade não estiver sediada no país, se o manuseio dos dados e a prestação de serviços e bens resultantes desse manuseio ocorrerem no território nacional, a legislação é válida. Da mesma forma, a legislação é pertinente se os dados pessoais sujeitos a tratamento tiverem sido coletados no território brasileiro.[244]

Ao examinar as principais disposições presentes no Regulamento Geral de Proteção de Dados e na Lei Geral de Proteção de Dados, torna-se evidente que a legislação brasileira se inspira fortemente no regulamento europeu. Isso inclui a implementação de uma legislação ampla sobre o assunto, a definição de direitos fundamentais para os detentores dos dados e o estabelecimento de uma autoridade supervisora independente.

Quanto às estratégias e aos dispositivos regulatórios estabelecidos em ambas as normativas, nota-se que os legisladores escolheram a mesma abordagem responsiva, fundamentada em uma governança nodal, para a implementação, aplicação e fiscalização mais eficaz dessas normas pelas autoridades regulatórias.[245]

A GDPR demanda que as entidades considerem a proteção de dados durante a etapa de idealização de novos produtos, serviços e projetos, conceituada como *privacy by design*. Isso decorre da compreensão de que a confidencialidade, desde o início, em conjunto com os elementos de responsabilidade organizacional e a abordagem de avaliação de riscos, constituem o alicerce essencial do quadro legal contemporâneo de privacidade de dados introduzido pela legislação europeia.

No que concerne à sua forma de aplicação, uma das principais inovações introduzidas pelo recente regulamento europeu foi a incorporação do princípio de responsabilização no art. 24,[246] exigindo que as entidades: adotem diretrizes, procedimentos e medidas para efetivar suas

---

[244] IRAMINA, A. RGPDv.LGPD: Adoção Estratégica da Abordagem Responsiva na Elaboração da Lei Geral de Proteção de Dados do Brasil e do Regulamento Geral de Proteção de Dados da União Europeia. *Revista de Direito, Estado e Telecomunicações*, Brasília, v. 12, nº 2, p. 91-117, outubro de 2020.

[245] *Ibidem*.

[246] Artigo 24 - Responsabilidade do responsável pelo tratamento:
1. Tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o presente regulamento. Essas medidas são revistas e atualizadas consoante as necessidades. [...]

exigências e sejam capazes de evidenciar tal efetivação. Para a autora, a responsabilidade promove o tratamento ético dos dados por organizações e viabiliza uma proteção significativa das informações para os indivíduos, por meio de práticas operacionais obrigatórias que abrangem os elementos cruciais de responsabilidade (por exemplo, avaliação de riscos, registro de processos, implementação de medidas de segurança etc.).

Dessa forma, considerando o artigo mencionado, é possível interpretar que a GDPR inclui também uma perspectiva de análise de riscos, nesta situação, que impele as entidades não apenas a avaliar os riscos de prejuízo aos indivíduos, do mesmo modo os ganhos relacionados a usos específicos de dados pessoais, permitindo a implementação de medidas de redução de riscos alinhadas à análise de custo/benefício realizada pela empresa.

Ainda, apesar de o Regulamento ser imediatamente vinculativo nos Estados Membros, é crucial que os países europeus implementem diversas medidas legislativas em nível nacional, especialmente para instituir e delegar competências às entidades nacionais de proteção de dados, tais como a autoridade para impor penalidades administrativas.[247]

Da mesma maneira que na legislação europeia, a LGPD emprega um formato de legislação abrangente, visando edificar uma estrutura regulatória para consolidar a temática de proteção de informações pessoais como uma esfera de políticas públicas. Esta esfera é composta por dispositivos legais, medidas punitivas e um órgão administrativo incumbido da execução e aplicação da lei.

Além disso, fundamentado nos *Fair Information Principles* e nas Diretrizes sobre a Proteção da Privacidade e Fluxos Transfronteiriços de Dados Pessoais da OCDE, a LGPD incorporou como princípios essenciais no que diz respeito ao manejo de dados. Da mesma forma que no regulamento europeu, a LGPD manifesta preocupação com o fortalecimento dos titulares de dados, proporcionando controle e escolha significativos sobre suas informações pessoais. Por exemplo, eles devem ser devidamente comunicados acerca do processamento de seus dados pessoais, e essa comunicação deve ser nítida, apropriada, de fácil acesso e transparente.[248]

A comparação entre a GDPR e a LGPD revela semelhanças e diferenças significativas em suas abordagens para a proteção da privacidade e segurança dos dados. Ambos os marcos legais foram desenvolvidos para lidar com os desafios crescentes associados ao tratamento de

[247] IRAMINA, A. RGPDv.LGPD: Adoção Estratégica da Abordagem Responsiva na Elaboração da Lei Geral de Proteção de Dados do Brasil e do Regulamento Geral de Proteção de Dados da União Europeia. *Revista de Direito, Estado e Telecomunicações*, Brasília, v. 12, nº 2, p. 91-117. Outubro de 2020.
[248] *Ibidem*.

informações pessoais na era digital. A contraposição entre as duas destaca a influência global das preocupações com a privacidade e destaca a diversidade nas abordagens adotadas por diferentes regiões para enfrentar esses desafios comuns. É fundamental para as organizações compreenderem as nuances específicas de cada regulamento ao moldar suas políticas e práticas de proteção de dados, especialmente em um cenário empresarial globalizado e interconectado.

Anteriormente mencionamos o instrumento da avaliação de impacto, neste momento iremos retomar o raciocínio apresentado. As análises de impacto, já reconhecidas na esfera ambiental e no âmbito da salvaguarda de dados pessoais em suas variedades de relatórios de repercussão ambiental e relatório de repercussão à proteção de dados pessoais, são ferramentas de gestão que surgiram para examinar as possíveis ramificações de uma iniciativa sobre interesses sociais relevantes.

A partir dessa avaliação, buscam respaldar um processo decisório embasado sobre se deve implementar a iniciativa e, em caso afirmativo, sob quais condições. São utilizadas em contextos nos quais existe incerteza em relação a eventos futuros, como na introdução de novas tecnologias. Por conseguinte, as análises são meios para produzir evidências a respeito das escolhas tomadas e para resguardar determinadas inquietações da sociedade.[249]

Desde já, é pertinente ressaltar que o mecanismo de avaliação de impacto se distingue de outras práticas corporativas, como uma avaliação de conformidade regulatória, devido à sua natureza precavida e preventiva. Sua finalidade é detectar riscos e implementar medidas de atenuação eficazes antes da adoção de uma específica tecnologia, seguindo uma análise pública que desencadeia um controle social e uma forma de governança em rede.

No contexto da cada vez mais frequente utilização de sistemas de inteligência artificial para automatizar tomadas de decisão em nosso dia a dia, isso está relacionado ao que se convencionou denominar de "devido processo informacional". Isso representa uma maneira de efetivar o contraditório e a ampla defesa e, por conseguinte, de restrição sobre ações que interfiram indevidamente em liberdades públicas - por exemplo, policiamento preditivo - e direitos individuais - por exemplo, liberdade de expressão no contexto de moderação de conteúdo, através de um maior controle sobre os procedimentos realizados.[250]

Além disso, é crucial salientar que a condução do mecanismo de avaliação de impacto deve ser encarada não como um ônus ou mera obrigação para o provedor, mas como uma

---

[249] BIONI, Bruno; GARROTE, Marina; GUEDES, Paula. *Temas centrais na Regulação de IA:* O local, o regional e o global na busca da interoperabilidade regulatória. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2023.
[250] *Ibidem*.

oportunidade. Dada a natureza dos produtos/serviços de IA e suas características e alcance, o modelo de avaliação sugerido pode auxiliar consideravelmente as empresas e outras entidades a criar IA centrada no ser humano e eficiente, mesmo em contextos desafiadores. Com isso, promover mais confiança, não apenas na tecnologia, mas também nas transações econômicas ao seu redor.

Finalmente, é crucial ressaltar que, mais relevante do que a simples antecipação de um instrumento de avaliação de impacto algorítmico, é sua devida proceduralização para se transformar em uma eficaz ferramenta de devido processo informacional e responsabilização. Como exemplo, o projeto de lei brasileiro PL 21/20 definiu, no art. 2º, VI, o que constituiria um relatório de impacto de inteligência artificial, entretanto, sem fornecer detalhes mais específicos sobre seus propósitos, prazos e parâmetros mínimos, gerando, assim, insegurança jurídica.[251]

Para os autores, a ausência de uma proceduralização mínima, ou seja, a organização do que deve constar nessa ferramenta (como prazos, critérios e metodologia escolhida), acarreta dificuldades para sua efetivação. Ao mesmo tempo, esse tipo de parametrização não deve ser excessivamente prescritivo para evitar a rigidez de uma ferramenta que precisa ser tão flexível quanto o desenvolvimento de tecnologias de IA e outras técnicas de tratamento de dados. Nesse sentido, é positivo que a futura regulamentação de IA estabeleça uma organização mínima, funcionando como uma espécie de base, para uma construção sólida de avaliação de impacto algorítmico. Em outras palavras, um patamar e não um limite para a modelagem dessa ferramenta essencial. Tais afirmações se harmonizam com o que temos argumentado aqui.

Defende-se que as Avaliações de Impacto em Direitos Humanos (AIA) relacionadas à inteligência artificial devem adotar essa perspectiva, ressaltando que a utilização da IA pode acarretar vantagens expressivas para a humanidade, para além de possíveis efeitos prejudiciais. A principal função das avaliações de impacto em direitos humanos deveria consistir em identificar potenciais riscos de violação desses direitos decorrentes de um sistema específico de IA, em vez de balanceá-los com eventuais impactos benéficos. Portanto, o equilíbrio entre vantagens e riscos não necessariamente faria parte da metodologia de avaliação de impacto, mas poderia contribuir para a avaliação de oportunidades quanto à implementação de sistemas de IA.

Em documento acerca de responsabilidade em Inteligência Artificial elaborado pela OCDE em 2023 destacou a presença de, no mínimo, 4 fases para administração de perigos de

[251] BIONI, Bruno; GARROTE, Marina; GUEDES, Paula. *Temas centrais na Regulação de IA*: O local, o regional e o global na busca da interoperabilidade regulatória. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2023.

sistemas de IA, que compreenderia: especificação (abrangendo escopo, contexto, participantes e critérios de análise), análise (reconhecimento dos perigos individuais e coletivos com base na gravidade x probabilidade), gestão dos riscos (ações de atenuação) e supervisão (acompanhamento e revisão).[252]

No contexto nacional, de maneira análoga, o Projeto de Lei 2338/2023 também estabelece uma abordagem com, no mínimo, quatro fases representadas pela organização, compreensão do perigo, redução desses perigos e observação (art. 24).[253]

Tal convergência sugere uma busca por padrões e princípios compartilhados no gerenciamento de riscos relacionados à IA em nível global e nacional. A inclusão desses elementos em documentos legais e orientações reflete o reconhecimento da necessidade de regulamentar e supervisionar o desenvolvimento e a implementação de sistemas de IA. A abordagem proativa, envolvendo especificação, análise, gestão e supervisão, demonstra a compreensão da complexidade e das implicações éticas associadas à IA, e visa promover o desenvolvimento responsável e sustentável dessa tecnologia.

Em 2018, a Comissão Europeia publicou um documento com diretrizes para o desenvolvimento ético da inteligência artificial, denominado "*Ethics guidelines for a trustworthy AI*". Este recebeu mais de quinhentos comentários e foi reformulado após isso. Em 2019, uma nova versão de mesmo nome foi publicada. A abordagem principiológica foi mantida, entretanto, é possível dividir uma inteligência artificial de confiança em três determinações gerais.

De acordo com a declaração ela deve ser: legal, ética e robusta. Por legal compreende-se respeitar todas as leis e regulamentações aplicáveis, em relação à ética, respeitar seus princípios e valores, e, finalmente, robusta está associada a uma perspectiva técnica levando em conta, ao mesmo tempo, o meio ambiente.

Em relação à transparência, o referido documento estabelece que é formada por quatro atributos. São eles: 1) Rastreabilidade dos dados: é crucial que os sistemas registrem e documentem todas as decisões tomadas no contexto da inteligência artificial; 2) Fundamentação: consiste na apresentação da explicação de todas as decisões e no processo que

---

[252] OECD. *Advancing accountability in AI:* Governing and managing risks throughout the lifecycle for trustworthy AI. 23 de fevereiro de 2023. Disponível em: https://www.oecd-ilibrary.org/science-and-technology/advancing-accountability-in-ai_2448f04b-en. Acesso em: 28 nov. 2023.

[253] Art. 24. A metodologia da avaliação de impacto conterá, ao menos, as seguintes etapas:
I – preparação;
II – cognição do risco;
III – mitigação dos riscos encontrados;
IV – monitoramento.

resultou nessas decisões por meio de algoritmos; 3) Comunicabilidade: refere-se à informação completa e adequada aos usuários sobre todas as capacidades e limitações dos sistemas de inteligência artificial; 4) Interatividade: identificar os responsáveis pelos sistemas para possibilitar uma interação com os usuários.[254]

A abordagem principiológica do documento, mantendo os princípios fundamentais, é uma estratégia consistente. A definição de uma IA confiável em três categorias - legal, ética e robusta - é uma maneira abrangente de abordar as dimensões complexas associadas ao desenvolvimento, implementação e regulamentação da IA.

A atenção à legalidade e ética, juntamente com a robustez técnica, sublinha a necessidade de uma abordagem abrangente para garantir que a IA seja desenvolvida e utilizada de maneira responsável. Essas diretrizes fornecem um arcabouço valioso para as organizações e desenvolvedores considerarem ao implementar a IA de forma responsável e confiável, assim como para legisladores utilizarem as considerações como escopo.

Em resumo, os regulamentos de proteção de dados como a GDPR e a LGPD têm um impacto significativo na forma como os sistemas de IA são projetados e implementados. Eles estabelecem padrões rigorosos para a coleta, processamento e proteção de dados pessoais, garantindo que a integridade e a privacidade dos indivíduos sejam preservadas, mesmo em um ambiente tecnológico em constante evolução.

Como tal, é imperativo que as organizações que desenvolvem e implementam tecnologias de IA estejam plenamente conscientes dessas leis e as incorporem em seu desenvolvimento para garantir a conformidade e, mais importante, respeitar os direitos fundamentais de privacidade dos indivíduos.

Enquanto as legislações de proteção de dados, como o GDPR na União Europeia e a LGPD no Brasil, representam avanços significativos na proteção da privacidade dos indivíduos, aplicá-las em sistemas de Inteligência Artificial enfrenta desafios e lacunas complexas. Estes desafios emergem devido à natureza inovadora e dinâmica da IA levantando questões principiológicas e necessidade de uma autoridade competente para supervisionar sua implementação.

Adaptar os princípios de proteção de dados para o contexto da IA é um entrave. A transparência, por exemplo, no contexto da inteligência artificial, é um princípio fundamental de proteção de dados. Dessa forma, permitir avaliações independentes dos sistemas de IA pode

---

[254] COMISSÃO EUROPEIA. *Ethics guidelines for a trustworthy* AI. High-level Expert Group on Artficial Intelligence, 2019. Disponível em: https://digitalstrategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai. Acesso em: 14 abr. 2023.

aumentar a transparência. A existência de partes externas analisando os algoritmos e processos pode ajudar a identificar problemas e fornecer sugestões para melhorias.

A incapacidade de compreender o processo decisório cria uma lacuna na confiança do público em relação à tecnologia e pode minar a aceitação geral da Inteligência Artificial em diversas esferas de aplicação. A busca por soluções que promovam a explicabilidade e a transparência nos algoritmos de IA é essencial para garantir que as decisões tomadas por essas ferramentas sejam justas, compreensíveis para todos os envolvidos e em conformidade com os princípios fundamentais e de proteção de dados.

Este capítulo destaca a importância da pseudonimização na preservação da privacidade dos dados em um contexto digital interligado. Ela proporciona uma camada adicional de segurança, preservando a utilidade dos dados para análises e pesquisas legítimas. A prática de tornar anônimos ou pseudonimizar dados sensíveis é essencial para treinar modelos de IA colaborativamente, garantindo o anonimato dos usuários originais.

A conformidade legal, especialmente com regulamentações como a LGPD e a GDPR, é enfatizada como crucial, requerendo estratégias que respeitem os direitos de privacidade. No entanto, são apontados desafios, como a reversibilidade dos dados pseudonimizados, e a necessidade de revisão constante das regulamentações diante da evolução tecnológica.

Consideramos que o equilíbrio entre inovação e proteção de direitos individuais na regulação da inteligência artificial é um desafio complexo. Destacamos aspectos como transparência nas práticas de IA, definição clara de limites sobre o uso de dados e a consideração de vieses nos algoritmos. O contexto específico em que as estratégias de tornar anônimos e pseudonimizar são aplicadas é crucial, pois a efetividade pode variar.

Embora essas práticas visem proteger a privacidade, elas não garantem total segurança contra brechas. A obtenção adequada de consentimento também é questionada quanto à compreensão dos usuários. Conclui-se que, embora a pseudonimização seja valiosa para a conformidade legal e a construção da confiança do público, é imperativo reconhecer suas limitações e considerar práticas adicionais para uma proteção robusta dos dados pessoais.

A análise da efetividade dessas práticas é um processo em constante evolução, exigindo uma abordagem proativa e ajustável diante das mudanças rápidas na tecnologia e ameaças no cenário digital contemporâneo.

Na segunda parte deste capítulo apontamos como a reidentificação representa uma ameaça significativa, onde dados aparentemente não identificáveis podem ser associados a informações externas, revelando a fonte original desses dados. Os avanços na inteligência

artificial, especialmente no aprendizado de máquina, permitiram que algoritmos identificassem padrões intricados, inclusive em dados inicialmente considerados anônimos.

Enfrentar esses desafios demanda uma abordagem abrangente. Além de aprimorar as técnicas de anonimização, é imperativo educar as partes envolvidas sobre os riscos da reidentificação, promovendo a conscientização como o primeiro passo para uma proteção mais eficaz. Adicionalmente, a implementação de políticas e regulamentações rigorosas é essencial para controlar a coleta e compartilhamento de dados.

As organizações devem investir em pesquisa contínua para desenvolver técnicas de anonimização mais avançadas e robustas, capazes de resistir aos rápidos avanços na análise de dados. Essa abordagem multifacetada visa fortalecer as defesas contra a reidentificação e proteger a privacidade dos dados.

Assim, a inteligência artificial contemporânea representa um conjunto de tecnologias com a notável capacidade de gerar outras inovações, novas técnicas e aplicações. Essa característica singular diferencia a IA de outras inovações lançadas no mercado. Importa ressaltar que o objetivo aqui não é se opor aos avanços científicos dessa tecnologia, mas sim estabelecer parâmetros para fundamentar a discussão sobre o tema.

Nesse contexto, a análise dos princípios de proteção de dados presentes nas legislações relacionadas à inteligência artificial emerge como um guia essencial. Essa abordagem visa focar nas preocupações evidenciadas ao longo deste trabalho, proporcionando uma base para avaliar e orientar o desenvolvimento e a implementação responsável da inteligência artificial. O intuito é, assim, promover a reflexão e a construção de direcionamentos que considerem tanto os benefícios quanto os desafios inerentes a essa tecnologia em constante evolução.

Em relação aos princípios fundamentais de proteção de dados, conforme estabelecidos pela LGPD. O princípio da finalidade requer que dados pessoais sejam coletados para propósitos específicos e legítimos na aplicação da inteligência artificial. A transparência sobre esses propósitos é crucial para que os usuários compreendam o uso de suas informações.

O princípio da minimização preconiza a coleta apenas dos dados estritamente necessários, reduzindo o risco de processamento excessivo. Estratégias como anonimização e pseudonimização são essenciais para buscar a eficácia dos algoritmos, preservando a privacidade.

O princípio da prestação de contas enfatiza a responsabilidade das organizações na conformidade com os princípios de proteção de dados ao desenvolver e operar algoritmos de IA de maneira ética. A adoção responsável desses princípios não apenas protege a privacidade dos dados, mas também fortalece a confiança dos usuários na tecnologia e em seus

desenvolvedores. Projetar sistemas de IA em conformidade com esses princípios requer uma abordagem multidisciplinar, integrando conhecimentos em ciência da computação, ética, legislação e segurança de dados.

Finalmente, na terceira parte, debatemos como os regulamentos de proteção de dados, como GDPR e LGPD, impactam a concepção e implementação de sistemas de IA ao estabelecerem padrões rigorosos para a coleta, processamento e proteção de dados pessoais. Essas leis asseguram a integridade e privacidade dos indivíduos em um ambiente tecnológico em constante evolução. Para garantir conformidade e respeitar os direitos fundamentais de privacidade, é crucial que as organizações que desenvolvem tecnologias de IA estejam plenamente cientes dessas legislações.

Embora representem avanços significativos na proteção da privacidade, aplicar regulamentações como GDPR e LGPD a sistemas de IA enfrenta desafios complexos. A adaptação dos princípios de proteção de dados para a tecnologia em questão, especialmente em questões de transparência, é um obstáculo. A busca por soluções que promovam a explicabilidade e transparência nos algoritmos de IA é essencial para construir confiança pública, assegurar decisões justas e estar em conformidade com os princípios fundamentais de proteção de dados.

CONSIDERAÇÕES FINAIS

Em síntese, ao longo deste trabalho, exploramos os primórdios da inteligência artificial, desde as visões pioneiras de Turing e sua influente proposta de teste até os avanços contemporâneos na área, ressaltando a notável contribuição de John McCarthy na nomenclatura da IA. Na segunda parte do primeiro capítulo, aprofundamo-nos no aprendizado de máquina, desmistificando o funcionamento das "*machine learning*" e seu aprofundamento em redes neurais artificiais, com o intuito de tornar acessíveis esses conceitos para leitores juristas e fomentar debates interdisciplinares.

Adentrando a esfera dos dados pessoais, examinamos sua evolução desde a origem, associada ao direito de privacidade, até seu reconhecimento como direito fundamental, evidenciando a relevância da Lei Geral de Proteção de Dados (LGPD). Destacamos a transformação do conceito de privacidade, inicialmente centrado no direito de ser deixado só, para uma abordagem mais abrangente, vinculada ao bem-estar social.

Exemplificamos implicações da coleta de dados, como o emblemático caso "Cambridge Analytica", e discutimos a ilusão de imparcialidade nas tecnologias automatizadas, sublinhando a necessidade de uma perspectiva crítica. Termos como "*profiling*" e "*data mining*" foram definidos, revelando a assimetria de poder na manipulação de dados em massa, destacando implicações nos direitos à privacidade e ressaltando a importância da transparência e da regulamentação, especialmente em relação à "*accountability*" e ao acesso às informações.

No capítulo subsequente, enfocamos a importância da pseudonimização na preservação da privacidade em um contexto digital interconectado. Destacamos desafios legais, como a reversibilidade dos dados pseudonimizados, e discutimos o delicado equilíbrio entre inovação e proteção de direitos na regulação da inteligência artificial. A ênfase recai sobre a transparência e limites no uso de dados, avaliando a eficácia dessas práticas e reconhecendo suas limitações, indicando a necessidade de medidas adicionais para garantir uma proteção robusta dos dados pessoais.

A segunda parte deste capítulo aborda a ameaça da reidentificação, sublinhando a importância da educação sobre seus riscos, a implementação de políticas rigorosas e a pesquisa contínua para o desenvolvimento de técnicas avançadas de anonimização. Destaca-se a capacidade singular da inteligência artificial em gerar inovações, enfatizando a importância da análise dos princípios de proteção de dados presentes em legislações relacionadas. A exploração dos princípios fundamentais da LGPD, como finalidade, minimização e prestação de contas, destaca a necessidade crucial de conformidade ética e de uma abordagem multidisciplinar.

Na última seção, discutimos como regulamentos como GDPR e LGPD impactam a concepção e implementação de sistemas de IA estabelecendo padrões rigorosos para a coleta, processamento e proteção de dados pessoais. A despeito dos avanços, ressaltamos desafios na adaptação desses princípios para a IA, especialmente no que diz respeito à transparência, reforçando a urgência de desenvolver soluções que promovam a explicabilidade e estejam em conformidade com os princípios fundamentais de proteção de dados.

Necessário observar que a discussão está longe de ser encerrada, tanto pelos Projetos de Lei em tramitação, quanto pelas evoluções tecnológicas que ocorrem em velocidade cada vez maior. Assim, concluímos este trabalho enfatizando a importância contínua da transparência algorítmica e interpretabilidade na regulação da inteligência artificial, reconhecendo a necessidade de constante evolução diante do dinamismo tecnológico e suas implicações.

REFERÊNCIAS

ABRUSIO, Juliana. *Proteção de dados na cultura do algoritmo*. Belo Horizonte: D'Plácido, 2020.

ALAKE, Richmond. *What AlexNet Brought To The World Of Deep Learning.* Towards Data Science, julho de 2020. Disponível em: https://towardsdatascience.com/what-alexnet-brought-to-the-world-of-deep-learning-46c7974b46fc. Acesso em: 15 abr. 2023.

ALPAC. *Languages and machines: computers in translation and linguistics.* A report by the Automatic Language Processing Advisory Committee, Division of Behavioral Sciences, National Academy of Sciences, National Research Council. 1966, Washington: National Academy of Sciences, National Research Council. Disponível em: https://nap.nationalacademies.org/resource/alpac_lm/ARC000005.pdf. Acesso em: 08 abr. 2023.

ALTMAN, Max. *Hoje na História:* 1996 - Kasparov derrota o computador Deep Blue da IBM. Opera Mundi, fevereiro de 2020. Disponível em: https://operamundi.uol.com.br/hoje-na-historia/9727/hoje-na-historia-1996-kasparov-derrota-o-computador-deep-blue-da-ibm. Acesso em: 08 abr. 2023.

ALVES, Marco Antônio Sousa; DE ANDRADE, Otávio Morato. Da "caixa-preta" à "caixa de vidro": o uso da explainable artificial intelligence (XAI) para reduzir a opacidade e enfrentar o enviesamento em modelos algorítmicos. *Direito Público*, v. 18, n. 100, 2021.

AMOROZO, Marcos. Congresso tem pelo menos 46 projetos de lei para regulamentar do uso de inteligência artificial. CNN, 18 de fevereiro de 2024. Disponível em: https://www.cnnbrasil.com.br/politica/congresso-tem-pelo-menos-46-projetos-de-lei-para-regulamentar-do-uso-de-inteligenciaartificial/#:~:text=O%20PL%20regulamenta%20conceitos%2C%20fundamentos,identificados%20por%20meio%20de%20avalia%C3%A7%C3%A3o.

API DO CLOUD VISION. *Vision AI.* Google cloud. Disponível em: https://cloud.google.com/vision?hl=pt-br#section-3. Acesso em: 15 abr. 2023.

ARAUJO, Valter Shuenquener de; ZULLO, Bruno Almeida; TORRES, Maurílio. Big data, algoritmos e inteligência artificial na administração pública: reflexões para a sua utilização em um ambiente democrático. A&C - Revista de Direito Administrativo & Constitucional, volume 20, nº 80. P. 258, setembro de 2020. *Revista de Direito Administrativo e Constitucional*. Disponível em: http://dx.doi.org/10.21056/aec.v20i80.1219. Acesso em: 10 jun. 2023.

ARBIX, Glauco. "Algoritmos não são inteligentes nem têm ética, nós temos": a transparência no centro da construção de uma ia ética. *In:* COZMAN, Fábio G.; PLONSKI, Guilherme Ary; NERI, Hugo. *Inteligência artificial:* avanços e tendências. São Paulo: Instituto de Estudos Avançados, 2021. Cap. 11. p. 260-284.

AZEVEDO, Cynthia Picolo Gonzaga de. BUARQUE, Gabriela. PEREIRA, José Renato Laranjeira de. *Nota Técnica ao Projeto de Lei nº 2338/2023.* Coalizão Direitos na Rede, agosto de 2023, p. 21-22.

BARRETO, Luiz; PREZOTO, Marcelo. *Introdução à sistemas especialistas.* 2010. 34 f. Dissertação (Mestrado) - Curso de Mestrado em Tecnologia Para Sistemas e Fenômenos Complexos, Faculdade de Tecnologia, Universidade Estadual de Campinas, Limeira, 2010.

BARROS, Thiago. *O que é Siri e como usar o comando de voz do iPhone?* TechTudo, fevereiro de 2013. Disponível em: https://www.techtudo.com.br/noticias/2013/02/o-que-e-siri.ghtml. Acesso em: 08 abr. 2023.

BARTH, Susanne; IONITA, Dan; HARTEL, Pieter. Understanding online privacy—a systematic review of privacy visualizations and privacy by design guidelines. *ACM Computing Surveys (CSUR)*, v. 55, n. 3, p. 1-37, 2022. Disponível em: https://doi.org/10.1145/3502288. Acesso em: 30 nov. 2023.

BHATIA, Manjari. *Google Fotos:* inteligência para armazenar, organizar e compartilhar suas memórias. Think with Google, maio de 2017. Disponível em: https://www.thinkwithgoogle.com/intl/pt-br/estrategias-de-marketing/apps-e-mobile/google-fotos-armazenar-organizar-e-compartilhar-memorias/. Acesso em: 15 abr. 2023.

BIONI, Bruno R. *Proteção de Dados Pessoais:* A Função e os Limites do Consentimento. 3ª edição. Rio de Janeiro: Forense, 2021.

BIONI, Bruno Ricardo; LUCIANO, Maria. O princípio da precaução na regulação da inteligência artificial: seriam as leis de proteção de dados o seu portal de entrada. *In:* FRAZÃO, Ana; MULHOLLAND, Caitlin. *Inteligência artificial e direito:* ética, regulação e responsabilidade. São Paulo: Thomson Reuters Brasil, p. 207-232, 2019.

BIONI, Bruno. Compreendendo o conceito de anonimização e dado anonimizado. Cadernos Jurídicos. São Paulo, v. 21, p. 191-201, 2020.

BIONI, Bruno; GARROTE, Marina; GUEDES, Paula. *Temas centrais na Regulação de IA:* O local, o regional e o global na busca da interoperabilidade regulatória. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2023.

BITTAR, Carlos Alberto. *Os direitos da personalidade.* 8ª edição. São Paulo: Saraiva, 2015.

BOCCIA, Sandra. *Como a inteligência artificial pode ajudar na seleção de talentos.* Época Negócios, junho de 2019. Disponível em: https://epocanegocios.globo.com/Tecnologia/notic.ia/2019/06/como-inteligencia-artificial-pode-ajudar-na-selecao-de-talentos.html. Acesso em: 09 abr. 2023.

BONAVIDES, Paulo. *Curso de direito constitucional.* 18ª edição. São Paulo: Malheiros, 2006.

BOSCO, Francesca *et al. Profiling technologies and fundamental rights and values:* regulatory challenges and perspectives from European Data Protection Authorities. Reforming European data protection law, 2014, p. 3-33, 2015. Disponível em: https://link.springer.com/chapter/10.1007/978-94-017-9385-8_1. Acesso em: 18 set. 2023.

BRASIL. Senado Federal. Projeto de Lei nº 2338 de 2023. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/157233#tramitacao_10494842. Acesso em: 3 mar. 2024.

BRASIL. CGTP. ANPD. Nota Técnica nº 16/2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/Nota_Tecnica_16ANPDIA.pdf. Acesso em: 6 mar. 2024.

BRASIL, Supremo Tribunal Federal. *Recurso Extraordinário 1055941*, Rel. Min. Dias Toffoli, Tribunal Pleno, julgado em 28.11.2019. DJe 6.10.2020.

BRASIL, Supremo Tribunal Federal. *Recurso Extraordinário 601314*, Rel. Min. Edson Fachin, Tribunal Pleno, julgado em 24.2.2016, DJe 16.9.2016.

BURG, Tamara; GALDINO, Manoel; SAKAI, Juliana. *Recomendações de governança:* Uso de inteligência artificial pelo poder público. Transparência Brasil. Fevereiro de 2020. P. 6. Disponível em: https://www.transparencia.org.br/downloads/publicacoes/Recomendacoes_Governanca_Uso_IA_PoderPublico.pdf. Acesso em: 10 jun. 2023.

COCKBURN, Iain M.; HENDERSON, Rebecca; STERN, Scott. The impact of artificial intelligence on innovation: An exploratory analysis. *In: The economics of artificial intelligence:* An agenda. University of Chicago Press, 2018. p. 115-146. p. 116 e 117.

COLOMBO, Cristiano; FACCHINI NETO, Eugênio. Mineração de dados e análise preditiva: reflexões sobre possíveis violações ao direito de privacidade na sociedade da informação e critérios para sua adequada implementação à luz do ordenamento brasileiro. *Revista de Direito, Governança e Novas Tecnologias*, Florianópolis, v. 3, n. 2, p. 59, 2 dez. 2017. Conselho Nacional de Pesquisa e Pós-Graduação em Direito - CONPEDI. Disponível em: http://dx.doi.org/10.26668/indexlawjournals/2526-0049/2017.v3i2.2345. Acesso em: 13 set. 2023.

COMISSÃO EUROPEIA. *Ethics guidelines for a trustworthy AI.* High-level Expert Group on Artficial Intelligence, 2019. Disponível em: https://digitalstrategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai. Acesso em: 14 abr. 2023.

CONSTÂNCIO, A. S.; CARVALHO, D. R.; TSUNODA, D. F. Computer vision applications in healthcare: a literature review augmented with natural language processing techniques. *Research, Society and Development,* vol. 11, nº 10. p. 12-13, 2022. Disponível em: https://doi.org/10.33448/rsd-v11i10.32942. Acesso em: 08 abr. 2023.

COUTO, Júlia Colleoni *et al*. New trends in big data profiling. *In: Science and Information Conference.* Cham: Springer International Publishing, 2022. p. 808-825. Disponível em: http://dx.doi.org/10.1007/978-3-031-10461-9_55. Acesso em: 14 set. 2023.

COUTTO FILHO, Milton B. do; SOUZA, Julio C. Stacchini de; SCHILLING, Marcus T. Sobre o problema da integração generalizada de dados. *Sba: Controle & Automação Sociedade Brasileira de Automatica*, v. 18, n. 1, p. 24-43, mar. 2007. Disponível em: http://dx.doi.org/10.1590/s0103-17592007000100003. Acesso em: 23 out. 2023.

CRUZ, Francisco Brito (Coord.); MASSARO, Heloisa; OLIVA, Thiago; BORGES, Ester. *Internet e eleições no Brasil:* diagnósticos e recomendações. 1ª edição, São Paulo: InternetLab, 2019. p. 26. Disponível em: https://www.internetlab.org.br/wp-content/uploads/2019/09/policy-infopol-26919_4.pdf. Acesso em: 05 mai. 2022.

DEGENHARD, J. *Number of YouTube users worldwide from 2019 to 2028.* Statista, junho de 2023. Disponível em: https://www.statista.com/forecasts/1144088/youtube-users-in-the-world. Acesso em: 08 jun. 2023.

DIAS, Guilherme. *Como eram os computadores e mainframes na década de 1980.* Tecmundo, julho de 2014. Disponível em: https://www.tecmundo.com.br/supercomputadores/58611-computadores-mainframes-decada-1980-falta-imagens.htm. Acesso em: 08 abr. 2023.

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

DONEDA, Danilo. *Da Privacidade à Proteção de Dados Pessoais:* Fundamentos da Lei Geral de Proteção de Dados. 3ª edição, São Paulo: Thomson Reuters Brasil, 2021.

DUVANEL, Talita. *Inteligência artificial é usada a sério na escrita de filmes e séries e levantam questões sobre autoria e criatividade.* O Globo, fevereiro de 2023. Disponível em: https://oglobo.globo.com/cultura/filmes/noticia/2023/02/inteligencia-artificial-e-usada-a-serio-na-escrita-de-filmes-e-series-e-levantam-questoes-sobre-autoria-e-criatividade.ghtml. Acesso em: 08 mai. 2023.

ÉPOCA NEGÓCIOS ONLINE. *Nestlé usa inteligência artificial para monitorar a felicidade das vacas.* Época Negócios, setembro de 2019. Disponível em: https://epocanegocios.globo.com/Tecnologia/noticia/2019/09/nestle-usa-inteligencia-artificial-para-monitorar-felicidade-das-vacas.html. Acesso em: 09 abr. 2023.

EYNG, Eduardo; SILVA, Flávio Vasconcelos da; PALð, Fernando; FILETI, Ana Maria Frattini. Neural network based control of an absorption column in the process of bioethanol production. *Brazilian Archives Of Biology And Technology*, vol. 52, nº 4, p. 961-972, agosto de 2009. FapUNIFESP (SciELO). Disponível em: http://dx.doi.org/10.1590/s1516-89132009000400020. Acesso em: 11 mai. 2023.

FACELI, Katti; LORENA, Ana C.; GAMA, João; *et al*. *Inteligência Artificial* - Uma Abordagem de Aprendizado de Máquina. São Paulo: Grupo GEN, 2021. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788521637509/. Acesso em: 09 mai. 2023.

FERNANDES, M. E.; NUZZI, A. P. E.; Grounds of the General Data Protection Law (LGPD): A narrative review. *Research, Society and Development*, v. 11, n. 12, p. e310111234247, 2022. DOI: 10.33448/rsd-v11i12.34247. Disponível em: https://rsdjournal.org/index.php/rsd/article/view/34247. Acesso em: 7 nov. 2023.

FERREIRA, Juliano Rodrigues *et al.* Mitigação dos Riscos à Privacidade através da Anonimização de Dados. *Revista Ibérica de Sistemas e Tecnologias de Informação*, n. E49, p. 573-585, 2022.

FLECK, Leandro *et al*. Redes neurais artificiais: Princípios básicos. *Revista Eletrônica Científica Inovação e Tecnologia*, vol. 1, nº 13, p. 47-57, 2016. Disponível em: http://dx.doi.org/10.3895/recit.v7i15.4330. Acesso em: 11 mai. 2023.

FRAGA, Renê. *O que é o Google Brain e por que é tão importante na inteligência artificial?* Google Discovery, fevereiro de 2023. Disponível em: https://googlediscovery.com/2023/02/20/o-que-e-o-google-brain-e-por-que-e-tao-importante-na-inteligencia-artificial/. Acesso em: 08 abr. 2023.

GONÇALVES, André Luiz Dias. *Primeiro PC da IBM foi lançado há 40 anos.* Tecmundo, agosto de 2021. Disponível em: https://www.tecmundo.com.br/produto/222975-primeiro-pc-ibm-lancado-ha-40-anos.htm. Acesso em: 08 abr. 2023.

GOODMAN, Bryce.; FLAXMAN, Seth. European Union Regulations on Algorithmic Decision-Making and a "Right to Explanation". *AI Magazine*, vol. 38, nº 3, 2017. p. 50-57. Disponível em: https://doi.org/10.1609/aimag.v38i3.2741. Acesso em: 11 abr. 2023.

GOOGLE RESEARCH. *Publication Database*. Disponível em: https://research.google/pubs/. Acesso em: 08 abr. 2023.

GUALTIERI, André. *Contribuição à Comissão de Juristas do Senado Federal sobre Inteligência Artificial.* Senado Federal, 2022. Disponível em: https://legis.senado.leg.br/comissoes/arquivos?ap=6916&codcol=2504. Acesso em: 13 abr. 2023.

HASSABIS, Demis; SULEYMAN, Mustafa; LEGG, Shane. *DeepMind's work in 2016:* a round-up. Google DeepMind, janeiro de 2017. Disponível em: https://www.deepmind.com/blog/deepminds-work-in-2016-a-round-up. Acesso em: 18 abr. 2023.

HERCULANO-HOUZEL, Suzana. Uma Breve História da Relação entre o Cérebro e a Mente. *In:* LENT, Roberto. *Neurociência:* da mente ao comportamento. São Paulo: Grupo Gen, 2008. Cap. 1, p. 2. Disponível em: https://app.minhabiblioteca.com.br/#/books/978-85-277-1994-0/. Acesso em: 09 abr. 2023.

HISTORY OF DATA SCIENCE. *Google Brain:* The Brains Behind Your Search Engine, março de 2021. Disponível em: https://www.historyofdatascience.com/google-brain-the-brains-behind-your-search-engine/. Acesso em: 08 abr. 2023.

IRAMINA, A. RGPDv.LGPD: Adoção Estratégica da Abordagem Responsiva na Elaboração da Lei Geral de Proteção de Dados do Brasil e do Regulamento Geral de Proteção de Dados da União Europeia. *Revista de Direito, Estado e Telecomunicações*, Brasília, v. 12, nº 2, p. 91-117. Outubro de 2020.

KAUFMAN, Dora. *Desmistificando a inteligência artificial.* São Paulo: Grupo Autêntica, 2022. Disponível em: https://app.minhabiblioteca.com.br/#/books/9786559281596/. Acesso em: 10 abr. 2023.

KAUFMAN, Dora; SANTAELLA, Lucia. O papel dos algoritmos de inteligência artificial nas redes sociais. *Revista Famecos*, volume 27, maio de 2020. EDIPUCRS. Disponível em: http://dx.doi.org/10.15448/1980-3729.2020.1.34074. Acesso em: 19 abr. 2023.

KRIZHEVSKY, Alex; SUTSKEVER, Ilya; HINTON, Geoffrey E. Imagenet classification with deep convolutional neural networks. *Communications of the ACM*, vol. 60, nº 6. p. 84-90, 2017. Disponível em: https://dl.acm.org/doi/abs/10.1145/3065386. Acesso em: 15 abr. 2023.

LASMAR ALMADA, M. A.; SOUZA DE ALBUQUERQUE MARANHÃO, J. Contribuições e Limites da Lei Geral de Proteção de Dados para a Regulação da Inteligência Artificial no Brasil. Direito Público, [S. l.], v. 20, n. 106, 2023. DOI: 10.11117/rdp.v20i106.6957. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/6957. Acesso em: 13 mar. 2024.

LEFKOWITZ, Melanie. *Professor's perceptron paved the way for AI* – 60 years too soon. Cornell Chronicle, setembro de 2019. Disponível em: https://news.cornell.edu/stories/2019/09/professors-perceptron-paved-way-ai-60-years-too-soon. Acesso em: 09 abr. 2023.

LESLIE, David; BURR, Christopher; AITKEN, Mhairi. KATELL, Michael. BRIGGS, Morgan. RINCON, Cami. Human Rights, *Democracy, and the Rule of Law Assurance Framework for AI Systems:* A Proposal. Setembro de 2021. Disponível em: http://dx.doi.org/10.2139/ssrn.4027875. Acesso em: 10 jun. 2023.

LESSIG, Lawrence. Privacy as Property. *The Johns Hopkins University Press*, Baltimore, vol. 69, nº 1, P. 247-269, setembro de 2002. Disponível em: https://www.jstor.org/stable/40971547. Acesso em: 15 abr. 2023.

LESSIG, Lawrence. The Law of the Horse: what cyberlaw might teach. *Harvard Law Review*, vol. 113, nº 2, P. 543-545, dezembro de 1999. Disponível em: http://dx.doi.org/10.2307/1342331. Acesso em: 13 mai. 2023.

LIMA, Isaías. *Inteligência Artificial.* São Paulo: Grupo GEN, 2014. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788595152724/. Acesso em: 09 abr. 2023.

MACHADO, Diego; DONEDA, Danilo. Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados. *Revista dos Tribunais*. vol. 998. Caderno Especial. p. 99-128.

MARANHÃO, Juliano Souza de Albuquerque; FLORÊNCIO, Juliana Abrusio; ALMADA, Marco. Inteligência artificial aplicada ao direito e o direito da inteligência artificial. Suprema: revista de estudos constitucionais, 2021, v. 1, n. 1, p. 154-180. Disponível em: https://hdl.handle.net/1814/71840. Acesso em: 07 mar. 2024.

MARTINS, Pedro. HOSNI, David. *O Livre Desenvolvimento da Identidade Pessoal em Meio Digital:* Para além da proteção da privacidade? (The Free Development of Personal Identity in the Digital Environment: Beyond the Privacy Protection?) (July 16, 2019).

MARTINS, Pedro; HOSNI, David. O Livre Desenvolvimento da Identidade Pessoal em meio ditigal: Para Além da Proteção da Privacidade?. *In:* PASQUOT, Fabrício Bertini; ANJOS, Lucas Costa dos; BRANDÃO, Luíza Couto Chaves. (Org.). *Políticas, Internet e Sociedade.* 1 ed. Belo Horizonte: IRIS, 2019, v. 1, p. 46-5. Disponível em: http://dx.doi.org/10.2139/ssrn.3464025. Acesso em: 12 set. 2023.

MASSENO, Manuel David. Das Consequências Jurídicas da Adesão do Brasil aos Princípios da OCDE Para a Inteligência Artificial, Especialmente Em Matéria De Proteção de Dados. *Campo Jurídico*, v. 8, n. 2, p. 113-122, 1 jul. 2020. Centro Universitário São Francisco de Barreiras. Disponível em: http://dx.doi.org/10.37497/revcampojur.v8i2.659. Acesso em: 26 nov. 2023.

MCCARTHY, J., MINSKY, M. L., ROCHESTER, N., SHANNON, C. E. (2006). A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence. *AI Magazine*, volume 27, nº 4, agosto de 1955. Disponível em: https://doi.org/10.1609/aimag.v27i4.1904. Acesso em: 07 abr. 2023.

MCCARTHY, John. Generality in artificial intelligence. *Communications of the ACM*, volume 30, nº 12, P. 1030-1035, 1987. Disponível em: https://dl.acm.org/doi/abs/10.1145/33447.33448. Acessado em 09 de abril de 2023.

MCCARTHY, John. *What is artificial intelligence?* Basic questions. Formal Reasoning Group, Stanford, p. 1-15, novembro de 2007. Disponível em: http://jmc.stanford.edu/articles/whatisai.html. Acesso em: 09 abr. 2023.

MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a história de um conceito. *Pensar - Revista de Ciências Jurídicas*, vol. 25, nº 4, 2020. p. 8-9. Disponível em: https://doi.org/10.5020/2317-2150.2020.10828. Acesso em: 3 jun. 2023.

META. *Como o Facebook está usando IA para melhorar as descrições de fotos para pessoas cegas ou com deficiência visual.* Disponível em: https://about.fb.com/br/news/2021/01/como-o-facebook-esta-usando-ia-para-melhorar-as-descricoes-de-fotos-para-pessoas-cegas-ou-com-deficiencia-visual/. Acesso em: 15 abr. 2023.

MNIH, Volodymyr *et al. Playing atari with deep reinforcement learning.* ArXiv preprint arXiv:1312.5602, 2013. Disponível em: https://arxiv.org/pdf/1312.5602v1.pdf. Acesso em: 18 abr. 2023.

NORVIG, Peter. RUSSEL, Stuart. *Inteligência Artificial.* São Paulo: Grupo GEN, 2013. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788595156104/. Acesso em: 09 abr. 2023.

OECD. *A OCDE e o Brasil:* Uma relação mutuamente benéfica. Disponível em: https://www.oecd.org/latin-america/paises/brasil-portugues/. Acesso em: 14 abr. 2023.

OECD. *About us.* Disponível em: https://www.oecd.org/about/. Acesso em: 14 abr. 2023.

OECD. *Advancing accountability in AI:* Governing and managing risks throughout the lifecycle for trustworthy AI. 23 de fevereiro de 2023. Disponível em: https://www.oecd-ilibrary.org/science-and-technology/advancing-accountability-in-ai_2448f04b-en. Acesso em: 28 nov. 2023.

OECD. *Recomendation of the Council on OECD Legal Instruments Artificial Intelligence.* Committe on Digital Economy Policy. 2019. Disponível em: https://legalinstruments.oecd.org/api/print?ids=648&lan=en. Acesso em: 14 abr. 2023.

OLIVEIRA, Natanael. *Spotify anuncia recurso que utiliza inteligência artificial para recomendar músicas*; entenda. CNN Brasil, fevereiro de 2023. Disponível em: https://www.cnnbrasil.com.br/economia/spotify-anuncia-recurso-que-utiliza-inteligencia-artificial-para-recomendar-musicas-entenda/. Acesso em: 08 abr. 2023.

OLIVEIRA FILHO, Eduardo Luiz de. *Re-Identificação de Dados Anonimizados:* considerações de privacidade e responsabilidade na mineração de prescrições médicas. 2020. 126 f. Dissertação (Mestrado) - Curso de Mestrado Profissional em Direito, Escola de Direito de São Paulo, Fundação Getulio Vargas, São Paulo, 2020. Disponível em: https://repositorio.fgv.br/items/c1d8dcb2-0ffe-4f7e-829d-bf242b5066d7. Acesso em: 28 out. 2023.

OMENA, Mateus. *Greve de atores de Hollywood chega ao fim com acordo entre sindicato e estúdios*. Exame, 08 de novembro de 2023. Disponível em: https://exame.com/pop/greve-de-atores-de-hollywood-chega-ao-fim-apos-sindicato-aprovar-acordo-com-estudios/. Acesso em: 29 nov. 2023.

OPENAI. *Introducing ChatGPT.* Disponível em: https://openai.com/blog/chatgpt. Acesso em: 08 mai. 2023.

PEQUENAS EMPRESAS GRANDES NEGÓCIOS. *Obra feita por inteligência artificial vence concurso de arte e causa polêmica entre artistas.* Globo. Disponível em: https://revistapegn.globo.com/Tecnologia/noticia/2022/09/obra-feita-por-inteligencia-artificial-vence-concurso-de-arte-e-causa-polemica-entre-artistas.html. Acesso em: 15 abr. 2023.

PEREIRA, José Renato L. de. Transparência pela cooperação: como a regulação responsiva pode auxiliar na promoção de sistemas de machine-learning inteligíveis. *Revista de Direito Setorial e Regulatório*, v. 7, nº 1, p. 194-223, maio-junho 2021.

PINHEIRO, Patricia Peck. *Proteção de dados pessoais:* Comentários à lei n. 13.709/2018-lgpd. Saraiva Educação SA, 2020.

POSSI, Ana Beatriz Benincasa Possi Benincasa. *O Que é Anonimização e Pseudoanonimização De Dados?* Instituto Avançado de Proteção de Dados, 2 de novembro de 2019. Disponível em: https://iapd.org.br/o-que-e-anonimizacao-e-pseudoanonimizacao-de-dados/. Acesso em: 23 out. 2023.

PRATA, Paula *et al.* Garantia de Privacidade Versus Utilidade dos Dados em Anonimização: um estudo no ensino superior. *Revista Ibérica de Sistemas e Tecnologias de Informação*, nº 40, p. 112-127, 2020.

RAMOS, André de C. Curso de Direitos Humanos. 9ª edição. São Paulo: Editora Saraiva, 2022. Disponível em: https://app.minhabiblioteca.com.br/#/books/9786553622456/. Acesso em: 11 jun. 2023.

RICHBOURG, Robert F. *Deep Learning:* Measure Twice, Cut Once. Institute for Defense Analyses, 2018. Disponível em: http://www.jstor.org/stable/resrep36394. Acesso em: 08 abr. 2023.

RÖHE, Anderson *et al. Contribuição à Consulta Pública sobre o Marco Regulatório da Inteligência Artificial.* Grupo de Pesquisa de Direito e Inovação (GEDI). Senado Federal, 2022. Disponível em: https://legis.senado.leg.br/comissoes/arquivos?ap=6916&codcol=2504. Acesso em: 13 abr. 2023.

SÁ, Yuri Vasconcelos de Almeida. *Desenvolvimento de aplicações IA* – robótica, imagem e visão computacional. São Paulo: Platos Soluções Educacionais S.A., 2021.

SANTINO, Renato. *Como a inteligência artificial está melhorando o teclado do seu celular.* Olhar Digital, outubro de 2015. Disponível em: https://olhardigital.com.br/2015/10/08/noticias/como-a-inteligencia-artificial-esta-melhorando-o-teclado-do-seu-celular/. Acesso em: 08 abr. 2023.

SCHERMER, Bart W. The limits of privacy in automated profiling and data mining. *Computer Law & Security Review*, vol. 27, nº 1, p. 45-52, 2011. Disponível em: https://doi.org/10.1016/j.clsr.2010.11.009. Acesso em: 12 jun. 2023.

SCIENCE RESEARCH COUNCIL. *Lighthill Report:* Artificial Intelligence: a paper symposium. Reino Unido, 1973.

SEARLE, John R. Minds, brains, and programs. B*ehavioral And Brain Sciences*, vol. 3, nº 3. p. 417-424, setembro de 1980. Cambridge University Press (CUP). Disponível em: http://dx.doi.org/10.1017/s0140525x00005756. Acesso em: 08 abr. 2023.

SELBST, Andrew D. POWLES, Julia. Meaningful Information and the Right to Explanation. *International Data Privacy Law*, vol. 7, nº 4, 2017. p. 233-242. Disponível em: https://ssrn.com/abstract=3039125. Acesso em: 11 abr. 2023.

SIAFAKAS, N. Do We Need a Hippocratic Oath for Artificial Intelligence Scientists? *AI Magazine*, vol. 42, nº 4, p. 57-61, 2022. Disponível em: https://ojs.aaai.org/aimagazine/index.php/aimagazine/article/view/15090. Acesso em: 11 abr. 2023.

SILVA, Alexandre Gonçalves *et al*. Avaliação de gordura corporal de pacientes por visão computacional: uma revisão sistemática. *Journal of Health Informatics*, vol. 12, nº 1, 2020. Disponível em: https://jhi.sbis.org.br/index.php/jhi-sbis/article/view/686. Acesso em: 08 abr. 2023.

SILVA, Leandro Augusto da; PERES, Sarajane M.; BOSCARIOLI, Clodis. *Introdução à Mineração de Dados* - Com Aplicações em R. São Paulo: Grupo GEN, 2016. p. 7. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788595155473/. Acesso em: 23 set. 2023.

SIMITIS, Spiros. Reviewing Privacy in an Information Society. *University Of Pennsylvania Law Review*, vol. 135, nº 3, p. 707-746, março de 1987. Disponível em: http://dx.doi.org/10.2307/3312079. Acesso em: 15 abr. 2023.

SINGH, Jatinder; WALDEN, Ian; CROWCROFT, Jon; BACON, Jean. Responsibility & Machine Learning: part of a process. *Ssrn Electronic Journal*, 2016. Elsevier BV. Disponível em: http://dx.doi.org/10.2139/ssrn.2860048. Acesso em: 10 abr. 2023.

SUN, Chen et al. GDPRxiv: Establishing the State of the Art in GDPR Enforcement. *Proceedings on Privacy Enhancing Technologies*, v. 4, p. 484-499, 2023.

TEBET, Simone. *Relatório legislativo à comissão de constituição, justiça e cidadania*. Brasília, 2019. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=7956536&ts=1647518557553&disposition=inline&_gl=1*1lu93t7*_ga*MTE1ODAxNDMzNy4xNjY2NTc4NTk5*_ga_CW3ZH25XMK*MTY4NjUyNTMxNy42LjAuMTY4NjUyNTMxNy4wLjAuMA. Acesso em: 11 jun. 2023.

TUREK, Matt. *Defense Advanced Research Project Agengy (DARPA)*. Disponível em: https://www.darpa.mil/program/explainable-artificial-intelligence. Acesso em: 11 abr. 2023.

TURING, Alan. Computing Machinery and Intelligence. *Mind*, volume LIX, nº 236, outubro de 1950. p. 433. Disponível em: https://www.jstor.org/stable/2251299. Acesso em: 07 abr. 2023.

TUTT, Andrew. An FDA for algorithms. *Administrative Law Review*, vol. 69, nº 1, P. 85, 2017. Disponível em: https://static1.squarespace.com/static/603ab50ab81d5532a0a4a42b/t/63cc0b15bd14d66a8db3d1c5/1674316568048/R_69-1-Andrew-Tutt.pdf. Acesso em: 10 abr. 2023.

UNIÃO EUROPEIA. *Regulamento (Ue) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, Relativo À Proteção das Pessoas Singulares no Que Diz Respeito Ao Tratamento de Dados Pessoais e À Livre Circulação Desses Dados e Que Revoga A Diretiva 95/46/Ce (Regulamento Geral Sobre A Proteção de Dados) nº 679, de 27 de abril de 2016. Jornal Oficial da União Europeia*. Estrasburgo, 04 maio 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016R0679&qid=1701988584822. Acesso em: 27 nov. 2023.

VALLIM, Marco Vinicius Bhering de Aguiar. *Inteligência Artificial Explicável Aplicada a Hemogramas como Suporte à Tomada de Decisão em Diagnósticos de COVID-19*. 2021. 99 f. Dissertação (Mestrado) - Curso de Mestrado em Engenharia Elétrica e Computação, Programa de Pós-graduação em Engenharia Elétrica e Computação, Universidade Presbiteriana Mackenzie, São Paulo, 2021.

VIEIRA, C. P. R.; DIGIAMPIETRI, L. A. A study about Explainable Articial Intelligence: using decision tree to explain SVM. *Revista Brasileira de Computação Aplicada*, v. 12, n. 1, p. 113-121, 2020. Disponível em: https://seer.upf.br/index.php/rbca/article/view/10247. Acesso em: 29 out. 2023.

WACHTER, Sandra; MITTELSTADT, Brent; FLORIDI, Luciano. Why a right to explanation of automated decision-making does not exist in the general data protection regulation. *International Data Privacy Law*, volume 7, nº 2, p. 76-99, 2017. Disponível em: https://ssrn.com/abstract=2903469. Acesso em: 11 abr. 2023.

WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. *Harvard Law Review*, vol. 4, nº 5, p. 193, dezembro de 1890. Disponível em: http://dx.doi.org/10.2307/1321160. Acesso em: 15 abr. 2023.

WOLFGANG, Hoffmann-Riem. *Teoria Geral do Direito Digital*. São Paulo: Grupo GEN, 2021. Disponível em: https://app.minhabiblioteca.com.br/#/books/9786559642267/. Acesso em: 28 set. 2023.