



Ingo Wolfgang Sarlet
Jeferson Ferreira Barbosa
Andressa de Bittencourt Siqueira
Emmanuel Rocha Reis
Orgs.

Inteligência artificial, proteção de dados e inovação na saúde

Anais do IX Seminário Internacional de
Direito, Tecnologia e Inovação

Arte da capa:
Gabrielle Bezerra Sales Sarlet



Editora Fundação Fênix

A obra coletiva que temos o privilégio de apresentar, reúne textos produzidos por discentes dos Programas de Pós-Graduação em Direito e bolsistas de Iniciação Científica, resultantes dos trabalhos apresentados perante banca examinadora em grupos de trabalho temáticos promovidos por ocasião do “IX Seminário Internacional de Direito, Tecnologia e Inovação: Inteligência artificial, proteção de dados e inovação na saúde”, realizado em auditórios e salas de aula sediados na Pontifícia Universidade Católica do Rio Grande do Sul, PUCRS, em Porto Alegre. O evento ocorreu do dia 07 ao dia 09.11.2022 e contou, durante os turnos da manhã e da noite, com conferências de destacados interlocutores com relação aos temas propostos. Nos turnos da tarde, ocorreram as apresentações de discentes em grupos de trabalho (GTs), perante bancas avaliadoras. Desejamos uma excelente leitura e reflexão, agradecendo pelo esforço de todos os autores e pelas valiosas contribuições.

Os Organizadores.



Editora Fundação Fênix



Inteligência artificial, proteção de dados e inovação na saúde

Anais do IX Seminário Internacional de Direito, Tecnologia e Inovação

Série Direito

Conselho Editorial

Editor

Ingo Wolfgang Sarlet

Conselho Científico – PPG Direito PUCRS

Gilberto Stürmer – Ingo Wolfgang Sarlet

Marco Felix Jobim – Paulo Antonio Caliendo Velloso da Silveira

Regina Linden Ruaro – Ricardo Lupion Garcia

Conselho Editorial Nacional

Adalberto de Souza Pasqualotto – PUCRS

Amanda Costa Thomé Travincas – Centro Universitário UNDB

Ana Elisa Liberatore Silva Bechara – USP

Ana Maria DÁvila Lopes – UNIFOR

Ana Paula Gonçalves Pereira de Barcellos – UERJ

Angélica Lucía Carlini – UNIP

Augusto Jaeger Júnior – UFRGS

Carlos Bolonha – UFRJ

Claudia Mansani Queda de Toledo – Centro Universitário Toledo de Ensino de Bauru

Cláudia Lima Marques – UFRGS

Clara Iglesias Keller – WZB Berlin Social Sciences Center e Instituto Brasileiro de Ensino

Desenvolvimento e Pesquisa – IDP

Danielle Pamplona – PUCRS

Daniel Antônio de Moraes Sarmento – UERJ

Daniel Wunder Hachem – PUCPR e UFPR

Daniel Mitidiero – UFRGS

Denise Pires Fincato – PUCRS

Draiton Gonzaga de Souza – PUCRS

Eugênio Facchini Neto – PUCRS

Elda Coelho de Azevedo Bussinguer – UniRio

Fabio Siebeneichler de Andrade – PUCRS

Fabiano Menke – UFRGS

Flavia Cristina Piovesan – PUC-SP

Gabriel de Jesus Tedesco Wedy – UNISINOS

Gabrielle Bezerra Sales Sarlet – PUCRS

Germano André Doederlein Schwartz – UNIRITTER

Gilmar Ferreira Mendes – Ministro do STF, Professor Titular do IDP e Professor aposentado da UNB

Gisele Cittadino – PUC-Rio

Gina Vidal Marcilio Pompeu – UNIFOR

Giovani Agostini Saavedra – Universidade Presbiteriana Mackenzie – SP

Guilherme Camargo Massaú – UFPel

Gustavo Osna – PUCRS

Hermes Zaneti Jr

Hermilio Pereira dos Santos Filho – PUCRS
Ivar Alberto Martins Hartmann – FGV Direito Rio
Jane Reis Gonçalves Pereira – UERJ
Juliana Neuenschwander Magalhães - UFRJ
Laura Schertel Mendes
Lilian Rose Lemos Rocha – Uniceub
Luis Alberto Reichelt – PUCRS
Luís Roberto Barroso – Ministro do STF, Professor Titular da UERJ, UNICEUB, Sênior Fellow na Harvard Kennedy School
Miriam Wimmer - IDP - Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa
Mônia Clarissa Hennig Leal – UNISC
Otavio Luiz Rodrigues Jr – USP
Patryck de Araújo Ayala – UFMT
Paulo Ricardo Schier - Unibrasil
Phillip Gil França - UNIVEL – PR
Richard Pae Kim – UNISA
Teresa Arruda Alvim – PUC-SP
Thadeu Weber – PUCRS

Conselho Editorial Internacional

Alexandra dos Santos Aragão – Universidade de Coimbra
Alvaro Avelino Sanchez Bravo – Universidade de Sevilha
Catarina Isabel Tomaz Santos Botelho – Universidade Católica Portuguesa
Carlos Blanco de Moraes – Universidade de Lisboa
Clara Iglesias Keller – WZB Berlin Social Sciences Center e Instituto Brasileiro de Ensino Desenvolvimento e Pesquisa – IDP
Cristina Maria de Gouveia Caldeira – Universidade Europeia
César Landa Arroyo – PUC de Lima, Peru
Elena Cecilia Alvites Alvites – Pontifícia Universidade Católica do Peru
Elena Alvites Alvites - PUCP
Francisco Pereira Coutinho – Universidade NOVA de Lisboa
Francisco Ballaguer Callejón – Universidade de Granada - Espanha
Fernando Fita Ortega - Universidade de Valência
Giuseppe Ludovico - Universidade de Milão
Gonzalo Aguilar Cavallo – Universidade de Talca
Jorge Pereira da Silva – Universidade Católica Portuguesa
José João Abrantes – Universidade NOVA de Lisboa
José María Porrás Ramirez – Universidade de Granada – Espanha
Manuel A Carneiro da Frada – Universidade do Porto
Paulo Mota Pinto – Universidade de Coimbra
Pedro Paulino Grandez Castro – Pontificia Universidad Católica del Peru
Richard Pae Kim – Professor do Curso de Mestrado em Direito Médico da UNSA
Víctor Bazán – Universidade Católica de Cuyo

**Ingo Wolfgang Sarlet
Jeferson Ferreira Barbosa
Andressa de Bittencourt Siqueira
Emmanuel Rocha Reis
Organizadores**

**Inteligência artificial, proteção de dados e inovação na saúde
Anais do IX Seminário Internacional de Direito, Tecnologia e Inovação**



Editora Fundação Fênix

Porto Alegre, 2023

Direção editorial: Ingo Wolfgang Sarlet
Diagramação: Editora Fundação Fênix
Concepção da Capa: Editora Fundação Fênix

O padrão ortográfico, o sistema de citações, as referências bibliográficas, o conteúdo e a revisão de cada capítulo são de inteira responsabilidade de seu respectivo autor.

Todas as obras publicadas pela Editora Fundação Fênix estão sob os direitos da Creative Commons 4.0 –
http://creativecommons.org/licenses/by/4.0/deed.pt_BR



Série Direito – 79

Catálogo na Fonte

I61 Inteligência artificial, proteção de dados e inovação na saúde [recurso eletrônico] / Ingo Wolfgang Sarlet ... [et al.] Organizadores. – Porto Alegre : Editora Fundação Fênix, 2023.
272 p. (Série Direito ; 79)

IX Seminário Internacional de Direito, Tecnologia e Inovação: Inteligência artificial, proteção de dados e inovação na saúde.

Demais organizadores: Jeferson Ferreira Barbosa, Andressa de Bittencourt Siqueira, Emmanuel Rocha Reis.

Disponível em: <<http://www.fundarfenix.com.br>>

ISBN 978-65-5460-055-2

DOI <https://doi.org/10.36592/9786554600552>

1. Direito. 2. Inteligência Artificial. 3. Proteção de dados. 4. Direito fundamental. 5. Saúde digital. I. Sarlet, Ingo Wolfgang (org.).

CDD: 340

Responsável pela catalogação: Lidiane Corrêa Souza Morschel CRB10/1721

A publicação da presente obra foi viabilizada com o apoio do Programa de Pós-Graduação em Direito – PUCRS.

Além disso, registram-se as demais fontes de fomento financeiro para a realização do evento que resultou nos textos publicados, designadamente, o IX Seminário Internacional de Direito, Tecnologia e Inovação: Inteligência artificial, proteção de dados e inovação na saúde:

Chamada MCTIC/CNPq Nº 28/2018 - Universal/Faixa C, do Ministério da Ciência, Tecnologia, Inovações e Comunicações – MCTIC e Conselho Nacional de Desenvolvimento Científico e Tecnológico – CNPq.

Centro de Estudos Europeus e Alemães – CDEA – PUCRS/UFRGS.

Instituições e Entidades Promotoras do IX Seminário Internacional de Direito, Tecnologia e Inovação:

Escola de Direito e Programa de Pós-Graduação em Direito da Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS)

Centro de Estudos Europeus e Alemães (CDEA)

Universidade Federal do Rio Grande do Sul (PPGD-UFRGS)

Grupo de Estudos e Pesquisa em Direitos Fundamentais - GEDF (PPGD-PUCRS)

Grupo de Pesquisa Inteligência Artificial e Direito (PPGD-PUCRS)

Grupo de Pesquisa em Governança Cooperativa, Compliance e Proteção de Dados (PPDG – MACKENZIE)

Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP)

INSPER - Instituto de Ensino e Pesquisa

Universidade do Oeste de Santa Catarina (UNOESC)

Observatório da Proteção de Dados da Universidade Nova de Lisboa

Privacy and Data Protection Center da Universidade Europeia de Lisboa

Universidade de Granada



Coordenação Geral do Evento

Prof. Dr. Ingo Wolfgang Sarlet

Comissão Científica

Prof. Dr. Ingo Wolfgang Sarlet
Prof. Dr. Giovanni Saavedra
Prof. Dr. Ivar Hartmann
Profa. Dra. Gabrielle Bezerra Sales Sarlet
Profa. Dra. Regina Ruaro
Profa. Dra. Laura Schertel Mendes
Prof. Dr. Vinicius Almada Mozetic
Prof. Dr. Francisco Coutinho
Profa. Dra. Cristina Caldeira
Prof. Dr. Antonio Perez Miras

Comissão Executiva

Dr. Jeferson Ferreira Barbosa
Dda Andressa de Bittencourt Siqueira
Ddo Emmanuel Rocha Reis
Ddo Lucas Reckziegel Weschenf
Ddo Ricardo L L Tatsch
Ddo Pedro Agão Filter

SUMÁRIO

APRESENTAÇÃO

Os Organizadores 15

1. A INOVAÇÃO NA SAÚDE NO BRASIL FRENTE ÀS POLÍTICAS DE DESENVOLVIMENTO PRODUTIVO

Amanda dos Santos Kronbauer 21

2. OS DESAFIOS ÉTICOS DAS INTELIGÊNCIAS ARTIFICIAIS NA ERA E NO PÓS-ERA DA LEI GERAL DE PROTEÇÃO DE DADOS

Ana Luiza Liz dos Santos

Lucas Moreschi Paulo 41

3. DA INTERRELAÇÃO ENTRE DIREITO, TECNOLOGIA E GOVERNANÇA NA PROTEÇÃO DE DADOS PESSOAIS

Ariel Augusto Lira de Moura

Bernardo Leandro Carvalho Costa 67

4. A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD) NA PERSPECTIVA DE UMA CONSTITUIÇÃO EM REDE

Bernardo Leandro Carvalho Costa

Ariel Augusto Lira de Moura 85

5. IMPARCIALIDADE DO ÓRGÃO JURISDICIONAL: CONCEITO E TRANSFORMAÇÕES NO CONTEXTO DAS NOVAS TECNOLOGIAS

Drieli de Quadros Klippel 105

6. O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS E A ESTRATÉGIA DE SAÚDE DIGITAL PARA O BRASIL: ANÁLISE DA APLICAÇÃO DA LGPD NO TRATAMENTO DE DADOS PESSOAIS NO SISTEMA E-SAÚDE

Emmanuel Rocha Reis

Ricardo Luís Lenz Tatsch 121

7. UM ESTUDO SOBRE INTELIGÊNCIA ARTIFICIAL E OS RISCOS PARA A SAÚDE DAS CRIANÇAS: PERCEPÇÕES INTERNACIONAIS NA UNICEF E NA WEF	
<i>Lucas Reckziegel Weschenfelder</i>	143
8. O DESAFIO DA REGULAÇÃO DA INTELIGÊNCIA ARTIFICIAL NA SAÚDE: ASPECTOS TÉCNICO-JURÍDICOS DA SEGURANÇA DAS INFORMAÇÕES	
<i>Maria Eugênia Londero Deggeroni</i>	167
9. "HOW DARE YOU"? OS LIMITES À LIBERDADE DE INOVAR E OS NOVOS PARADIGMAS AO ESTUDO DO DIREITO CRIMINAL E DA GESTÃO EM SEGURANÇA PÚBLICA	
<i>Nathália Igisk Lopes Portuguese</i>	189
10. TELETRIAGEM NA TELESSAÚDE (TELEMEDICINA E TELEENFERMAGEM) POR INTELIGÊNCIA ARTIFICIAL: UM OLHAR PARA OS MARCOS REGULATÓRIOS NO BRASIL	
<i>Regina Linden Ruaro</i>	
<i>Helen Lentz Ribeiro Bernasiuk</i>	213
11. A GARANTIA DO DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS NEURAIS NO BRASIL: DESAFIOS E PERSPECTIVAS	
<i>Silvana Sampaio Arguelho</i>	
<i>Fernando Medici</i>	
<i>Giovani Agostini Saavedra</i>	235
12. SAÚDE PLANETÁRIA, EXTRAFISCALIDADE E O MANEJO DOS RESÍDUOS SÓLIDOS URBANOS	
<i>Victória Maltchik Salles Jung</i>	257

APRESENTAÇÃO

A obra coletiva que temos o privilégio de apresentar, reúne textos produzidos por discentes dos Programas de Pós-Graduação em Direito e bolsistas de Iniciação Científica, resultantes dos trabalhos apresentados perante banca examinadora em grupos de trabalho temáticos promovidos por ocasião do "IX Seminário Internacional de Direito, Tecnologia e Inovação: Inteligência artificial, proteção de dados e inovação na saúde", realizado em auditórios e salas de aula sediados na Pontifícia Universidade Católica do Rio Grande do Sul, PUCRS, em Porto Alegre.

O evento ocorreu do dia 07 ao dia 09.11.2022 e contou, durante os turnos da manhã e da noite, com conferências de destacados interlocutores com relação aos temas propostos. Nos turnos da tarde, ocorreram as apresentações de discentes em grupos de trabalho (GTs), perante bancas avaliadoras.

Com relação às conferências no dia 07.11.2022, a partir das 10h da manhã as atividades iniciaram com a abertura realizada pelo Prof. Dr. Ingo Sarlet e seguida pelas conferências do Prof. Dr. Fabricio Pozzebon (PUCRS), sobre "racismo algorítmico na datacracia"; da Profa. Dra. Temis Limberger (Unisinos), sobre "pós-pandemia e seus impactos na administração pública em rede"; do Prof. Dr. Paulo Caliendo (PUCRS), sobre "IA, tributação e financiamento da saúde". A presidência ficou a cargo do Prof. Dr. Ingo Wolfgang Sarlet. A partir das 19h ocorreram as conferências do Prof. Dr. Giacomo Palombino, sobre "la opinión del representante político en la época de la inteligencia artificial (online)"; do Prof. Dr. Ivar Hartmann (Insper), sobre "regulação da IA na América Latina: desafios e soluções comuns"; da Profa. Dra. Cristina Caldeira (Universidade Europeia), sobre "proteção de dados, saúde e novas tecnologias".

No dia 08.11.2022, a partir das 10h da manhã, ocorreram as apresentações do Prof. Dr. Rafael Bordini (Politécnica PUCRS), sobre "pesquisa e inovação em inteligência artificial aplicada à saúde"; da Profa. Dra. Gabrielle Sales Sarlet (PUCRS), sobre "IA e regulação no Brasil"; da Profa. Dra. Marcia Santana Fernandes (HCPA), sobre "AI e sua aplicação na saúde: uma retrospectiva histórica e desafios"; do Prof. Dr. Fabiano Menke (UFRGS), sobre "transferência internacional de dados pessoais". A presidência foi exercida pela Profa. Dra. Regina Linden Ruaro (PUCRS).

16 | Inteligência artificial, proteção de dados e inovação na saúde

Em 09.11.2022, a partir das 10h da manhã, as discussões foram impulsionadas pela Profa. Dra. Miriam Wimmer (IDP) a respeito dos “parâmetros para a participação humana em decisões de IA - entre a legitimidade e a eficiência” (online); pelo Prof. Dr. Francisco Pereira Coutinho (NOVA School of Law), sobre “o direito de não sujeição a decisões individuais automatizadas no Regulamento Geral de Proteção de Dados”; pelo Prof. Dr. Marco Aurélio Cruz (UFPEL), sobre “a concepção personalista da LGPD e as decisões tomadas unicamente com base em tratamento automatizado de dados pessoais”; pelo Prof. Dr. Giovani Saavedra (Mackenzie), a respeito da “compliance digital no setor da saúde” e pela Profa. Dra. Juliana Abrusio (Mackenzie), sobre “proteção de dados e consentimento”. A Profa. Dra. Regina Linden Ruaro (PUCRS) presidiu os trabalhos.

Tanto o evento quanto a presente publicação tem como objetivo promover um espaço aberto à comunidade acadêmica para reflexão e debate sobre as questões relacionadas ao tema “direito, tecnologia e inovação” especialmente quanto ao uso de inteligência artificial e dos impactos do mundo digitalizado à proteção de dados, estimulando o aperfeiçoamento do pensamento científico e a ampliação do conhecimento acerca dos impactos que as novas tecnologias geram no sistema jurídico, especialmente na seara dos direitos fundamentais, bem como a tensão entre tecnologia e sociedade. Com a finalidade de melhor organização e de otimizar os resultados, as conferências e os capítulos da presente obra se enquadram dentro de três linhas de pesquisa específicas: 1- inteligência artificial, proteção de dados e inovação na saúde; 2- inovação, segurança tecnológica e regulação na saúde e 3 - tecnologia, jurisdição e processo.

Nessa perspectiva temos então os doze trabalhos que compõe a presente obra. No primeiro capítulo o texto de Amanda dos Santos Kronbauer sobre “a inovação na saúde no Brasil frente às políticas de desenvolvimento produtivo” (PDPs), com o objetivo de “verificar como ocorre a inovação tecnológica na saúde no Brasil, na lógica das PDPs; em caráter específico, busca-se avaliar as parcerias dos setores público e privado para o desenvolvimento tecnológico na saúde do Brasil, mormente com relação aos medicamentos desenvolvidos no país em caráter de colaboração e por vezes cofinanciamento e posteriormente adotados pelo Sistema Único de Saúde”. Na sequência, Ana Luiza Liz dos Santos e Lucas Moreschi Paulo

abordam “os desafios éticos das inteligências artificiais na era e no pós-era da Lei Geral de Proteção de Dados”. Eles se propõem “pesquisar de que forma a ética, em sentido amplo, é capaz de evitar e combater discriminações em sistemas de inteligência artificial. Os objetivos específicos alcançam o estudo da ética e da responsabilidade na criação e no treinamento de algoritmos; a análise de como os algoritmos podem recair em decisões discriminatórias e injustas; também a análise de como efetivar a transparência e o accountability em sistemas de inteligência artificial; e a busca por parâmetros para a construção de uma inteligência artificial mais ética e transparente à luz do que dispõe a Lei Geral de Proteção de Dados brasileira”. Dando continuidade, Ariel Augusto Lira de Moura e Bernardo Leandro Carvalho Costa auxiliam na compreensão acerca “da interrelação entre direito, tecnologia e governança na proteção de dados pessoais”. Partindo do problema relativo a “como integrar conjuntamente o vínculo entre direito e tecnologia na governança da proteção de dados pessoais”, busca identificar as relações existentes dentro dos temas de pesquisa, particularmente no contexto da Lei Geral de Proteção de Dados (LGPD).

Bernardo Leandro Carvalho Costa e Ariel Augusto Lira de Moura abordam a Lei Geral de Proteção de Dados na perspectiva de uma constituição em rede. Eles têm como objetivos “apresentar o contexto de surgimento da Lei Geral de Proteção de Dados (LGPD), destacando sua inclusão em um processo transnacional de regulamentações sobre o tema, impulsionado pela Organização para a Cooperação e Desenvolvimento (OCDE)”. Drieli de Quadros Klippel, no quinto capítulo, trata da “imparcialidade do órgão jurisdicional: conceito e transformações no contexto das novas tecnologias”. A autora “busca analisar, a partir do direito fundamental à imparcialidade do julgador e o avanço das novas tecnologias no processo, o impacto dos vieses comportamentais nas decisões judiciais. Ainda, se é possível e em que medida é possível empregar a inteligência artificial como ferramenta voltada ao proferimento de decisões judiciais mais justas e imparciais, sem que haja presença de vieses comportamentais dos julgadores”. Logo após, no capítulo 6, a temática “o direito fundamental à proteção de dados pessoais e a estratégia de saúde digital para o Brasil: análise da aplicação da LGPD no tratamento de dados pessoais no sistema e-saúde” é apresentada por Emmanuel Rocha Reis e por Ricardo Luís Lenz Tatsch.

No trabalho “apresenta-se a problemática do tratamento de dados pessoais sensíveis na política nacional da saúde digital e possíveis limites no seu uso, considerando a diversidade de atores e dos interesses das organizações presentes no complexo processo da saúde brasileira, apresentando interseções da LGPD diante das fragilidades do sistema e buscando um parâmetro limitador para o uso desses dados”.

No capítulo 7 temos “um estudo sobre inteligência artificial e os riscos para a saúde das crianças: percepções internacionais na UNICEF e na WEF”, que é apresentado por Lucas Reckziegel Weschenfelder. “O texto apresenta uma síntese das iniciativas relacionadas às aplicações de inteligência artificial, e seus riscos para a saúde das crianças, em sede de UNICEF e de WEF”. Continuando no campo relacionado à saúde temos o estudo de Maria Eugênia Londero Deggeroni intitulado “o desafio da regulação da inteligência artificial na saúde: aspectos técnico-jurídicos da segurança das informações”. A pesquisadora “aborda as limitações da regulação da inteligência artificial na saúde, frente as medidas de cibersegurança, com o questionamento: observando o padrão específico e o ordenamento jurídico brasileiro, quais as medidas técnicas a serem tomadas no âmbito da inteligência artificial na saúde?”. Com isso busca “estabelecer meios de proteção para que a inteligência artificial não seja uma fragilidade, ainda mais no caso dos dados de saúde.” Já o capítulo seguinte estabelece uma intersecção com o direito criminal. Nathália Igisk Lopes Portuguese se propõe ao estudo denominado “‘How dare you’? os limites à liberdade de inovar e os novos paradigmas ao estudo do direito criminal e da gestão em segurança pública’. Para ela “se os processos científicos de inovação se revelarem de maneira transcendente ao desenvolvimento social, absorvendo o homem e não sendo por ele absorvido, demonstra-se a fundamentalidade de ser traçar os limites de sua atuação, freando a emancipação de ferramentas que devem estar a nosso serviço e não contra nós”. Assim, foca a sua análise “sobre o confronto Segurança Pública versus Inovação, oferecendo a compatibilização entre ambos contra a mútua aniquilação”.

A “teletriagem na telessaúde (telemedicina e telenfermagem) por inteligência artificial: um olhar para os marcos regulatórios no Brasil” ganha a atenção de Regina Linden Ruaro e de Helen Lentz Ribeiro Bernasiuk. O objetivo geral do estudo é

“analisar a necessidade de regulamentação, em nível nacional, no tocante ao uso de sistemas de IA para triagem em telessaúde, no contexto da Telemedicina e Telenfermagem no Brasil; os objetivos específicos, por sua vez, desdobram-se em: (a) compreender a aplicabilidade de inteligência artificial à triagem em telemedicina; (b) verificar marcos regulatórios da telemedicina e telenfermagem no Brasil; (c) analisar necessidades de regulamentação, em nível nacional, no tocante ao uso de sistemas de IA para triagem em telemedicina por planos de saúde privados e Sistema Único de Saúde – SUS”. Silvana Sampaio Arguelho e Fernando Medici apresentam o tema: “a garantia do direito fundamental à proteção de dados neurais no Brasil: desafios e perspectivas”. “Inúmeros são os desafios éticos e jurídicos relacionados à privacidade e à autonomia dos indivíduos a serem enfrentados na era digital, incluída aqui a possibilidade de implementação de mecanismos de controle e transparência no uso da neurotecnologia”. Por ser um assunto ainda pouco explorado, o trabalho pretende “investigar a atual situação regulatória da proteção da mente em nível internacional e as iniciativas em andamento no âmbito nacional”. No capítulo 12, Victória Maltchik Salles Jung enfoca a “saúde planetária, extrafiscalidade e o manejo dos resíduos sólidos urbanos”. O trabalho busca “verificar como a extrafiscalidade pode auxiliar no correto manejo dos resíduos sólidos, atenuando a proliferação de doenças. A relevância do tema surge a partir do entendimento de que o direito à saúde, mesmo disposto no capítulo dos direitos sociais da Constituição Federal de 1988, pode ser lido enquanto um direito fundamental, mediante interpretação extensiva do direito à vida. A hipótese lançada é que a extrafiscalidade aparece como um forte estímulo às práticas sustentáveis na gestão do lixo, efetivando a promoção do direito fundamental à saúde,” investigado, mais especificamente, no âmbito coletivo.

Ao concluir a apresentação, desejamos uma excelente leitura e reflexão, agradecendo pelo esforço de todos os autores e pelas valiosas contribuições.

Ingo Wolfgang Sarlet.

Jeferson Ferreira Barbosa.

Andressa de Bittencourt Siqueira.

Emmanuel Rocha Reis.

1. A INOVAÇÃO NA SAÚDE NO BRASIL FRENTE ÀS POLÍTICAS DE DESENVOLVIMENTO PRODUTIVO

INNOVATION IN HEALTH IN BRAZIL IN THE FACE OF PRODUCTIVE DEVELOPMENT POLICIES (PDPs)



<https://doi.org/10.36592/9786554600552-01>

Amanda dos Santos Kronbauer¹

RESUMO

A saúde foi consagrada como direito social pelo art. 6º da Constituição Cidadã de 1988. O objetivo geral do presente trabalho é verificar como ocorre a inovação tecnológica na saúde no Brasil, na lógica das PDPs; em caráter específico, busca-se avaliar as parcerias dos setores público e privado para o desenvolvimento tecnológico na saúde do Brasil, mormente com relação aos medicamentos desenvolvidos no país em caráter de colaboração e por vezes co-financiamento e posteriormente adotados pelo Sistema Único de Saúde. Os métodos de abordagem utilizados foram o dedutivo e o sistêmico, ao passo que os métodos de procedimentos adotados foram o histórico e o tipológico. Os resultados parciais encontrados foram no sentido de que a inovação é necessária, de que a parceria entre os setores público e privado é benéfica para a sociedade e de que as políticas de desenvolvimento produtivo na saúde terão sucesso somente se forem implementadas com base nos princípios legais previstos na legislação brasileira vigente.

Palavras-chave: saúde no Brasil; PDP; inovação; parceria público-privada; SUS.

ABSTRACT

Health was enshrined as a social right by article 6 of the 1988 Constitution. The general objective of the present study is to verify how technological innovation occurs in the health sector in Brazil, according to the logic of PDPs; as an specific

¹ Mestranda em Direito (PUCRS); <http://lattes.cnpq.br/1845383903675561>; amanda.kronbauer@hotmail.com

objective, it seeks to evaluate the partnerships of the public and private sectors for the technological development in health in Brazil, especially regarding the medicines developed in the country in a collaborative character and sometimes co-financing and later adopted by the Unified Health System. The methods of approach used were deductive and systemic, while the methods of procedures adopted were historical and typological. The partial results found were in the sense that innovation is necessary, that the partnership between the public and private sectors is beneficial to society and that productive development policies in health will succeed only if they are implemented based on the legal principles provided for in the current Brazilian legislation.

Keywords: health in Brazil; PDP; innovation; public-private partnership; SUS.

1. INTRODUÇÃO

As fragilidades verificadas no campo da inovação tecnológica brasileira constituem um quadro de vulnerabilidade do sistema de saúde que consiste basicamente no risco que a sociedade brasileira corre por não ter condições suficientes de produzir medicamentos e garantir acesso adequado às demandas da população, e assim depender excessivamente de fornecedores internacionais (GADELHA, 2005).

Logo, visando reduzir estas vulnerabilidades e, de acordo com as diretrizes das políticas públicas relacionadas, é possível por meio de uma coordenação de diversos instrumentos de fomento ao Estado, aumentar a produção industrial e os esforços de inovação no país de forma a assegurar, a médio e longo prazos, o fornecimento seguro de produtos.

A transferência de tecnologia tem sido uma importante medida que prevê o desenvolvimento e inovação dos laboratórios públicos, uma vez que as parcerias envolvem a produção de medicamentos de alto valor agregado e atuais objetos de importações. Algumas das parcerias envolvem produtos biológicos e obtidos por fermentação, tecnologias ainda incipientes no país e utilizadas para produzir medicamentos para o tratamento de doenças como o câncer e doenças genéticas (REZENDE, 2013).

O objetivo geral, portanto, é verificar como ocorre a inovação tecnológica na saúde no Brasil, na lógica das PDPs. Em caráter específico, busca-se avaliar as parcerias dos setores público e privado para o desenvolvimento tecnológico na saúde do Brasil, mormente com relação aos medicamentos desenvolvidos no país em caráter de colaboração e por vezes co-financiamento e posteriormente adotados pelo Sistema Único de Saúde.

Os métodos de abordagem utilizados são o dedutivo, em uma análise do geral para o particular, e o sistêmico, considerando que os elementos podem ser reunidos em um conjunto na mesma ordem organizativa, levando-se em conta sua interação com o contexto histórico-econômico.

Os métodos de procedimentos adotados são o histórico, investigando acontecimentos e visões passadas para verificar sua influência na contemporaneidade, e o tipológico, dada a comparação de fenômenos sociais complexos. O método de interpretação é o exegético, visando descobrir o espírito do legislador, presente no texto legal.

Assim, o escopo do presente trabalho é investigar se é benéfica a transferência de tecnologia, desenvolvimento e produção nacional de insumos farmacêuticos, medicamentos, produtos para saúde e kits diagnóstico, adotadas por meio das Políticas de Desenvolvimento Produtivo (PDPS).

2. AS POLÍTICAS DE DESENVOLVIMENTO PRODUTIVO

O desenvolvimento produtivo pode ser entendido como um processo de transformação da economia, que visa ampliar a capacidade produtiva e a competitividade das empresas. Nesse sentido, é importante destacar que o desenvolvimento produtivo não se trata apenas de um aumento da produção, mas sim de uma transformação qualitativa e sustentável da economia, que combina inovação tecnológica, melhoria da eficiência produtiva e qualidade dos produtos e serviços.

Para alcançar o desenvolvimento produtivo, é necessário que haja um ambiente propício ao investimento e à inovação, além de políticas públicas que incentivem o empreendedorismo e a competitividade das empresas. É nesse

contexto que surgem as políticas de desenvolvimento produtivo, que têm como objetivo criar um ambiente favorável ao crescimento econômico e à geração de empregos.

2.1 DAS PARCERIAS ENTRE OS SETORES PÚBLICO E PRIVADO

As políticas de desenvolvimento produtivo têm sido uma das principais estratégias utilizadas pelos governos para promover o crescimento econômico, a geração de empregos e o aumento da competitividade das empresas. O objetivo dessas políticas é estimular a inovação tecnológica, melhorar a eficiência produtiva e aumentar a qualificação da mão de obra, entre outras medidas. Nesse sentido, é fundamental compreender as parcerias entre os setores público e privado na implementação dessas políticas.

Para colocar em prática essas políticas, os governos buscam parcerias com o setor privado, visando a complementariedade de esforços e recursos. No entanto, a relação entre o setor público e o privado nem sempre é harmoniosa, havendo conflitos de interesse, disputas por recursos e divergências de opinião quanto ao direcionamento das políticas de desenvolvimento produtivo. As parcerias entre os setores público e privado são fundamentais para o sucesso das políticas de desenvolvimento produtivo. O governo tem o papel de criar um ambiente favorável ao investimento e à inovação, enquanto as empresas têm a responsabilidade de investir em tecnologia e capacitação empresarial (NIKOLIC; MAIKISCH, 2006).

A parceria entre o setor público e privado na promoção do desenvolvimento produtivo tem sido objeto de discussão em diversos países, cada um com suas particularidades. No Brasil, por exemplo, a Lei de Inovação (Lei nº 10.973/2004) estabelece as bases legais para a cooperação entre empresas e instituições de pesquisa e desenvolvimento, com o objetivo de estimular a inovação tecnológica e o aumento da competitividade.

A Lei de Inovação prevê a possibilidade de celebração de contratos de transferência de tecnologia entre empresas e instituições de pesquisa, além da criação de incubadoras de empresas, parques tecnológicos e outras iniciativas de fomento à inovação.

Outro exemplo no mesmo sentido é a Coreia do Sul, que implementou uma política de desenvolvimento produtivo baseada na cooperação entre o Estado e as grandes empresas do país, conhecida como chaebol. Nesse modelo, o governo coreano ofereceu incentivos fiscais e financeiros às empresas que se comprometeram a investir em áreas consideradas prioritárias para o desenvolvimento econômico, como a produção de semicondutores e a tecnologia da informação (NIKOLIC; MAIKISCH, 2006).

As parcerias entre o setor público e privado na promoção do desenvolvimento produtivo podem apresentar vantagens e desvantagens para ambos os lados. Para o setor público, as vantagens podem incluir a ampliação das possibilidades de captação de recursos e a redução dos custos de investimento em infraestrutura e tecnologia (SCHMIDT; ASSIS, 2011). Já para o setor privado, as vantagens podem ser a obtenção de benefícios fiscais e financeiros, além da oportunidade de participar de projetos de grande escala e contribuir para o desenvolvimento econômico do país (FREEMAN, 2001).

No entanto, as parcerias também podem apresentar riscos e desafios, como a necessidade de compatibilização de interesses e objetivos, além da garantia da transparência e da legalidade dos processos envolvidos. Em termos jurídicos, há diversas questões que devem ser consideradas na análise das parcerias público-privadas em prol do desenvolvimento produtivo, como veremos adiante.

2.2 ASPECTOS JURÍDICOS RELEVANTES DAS PDPs

As políticas de desenvolvimento produtivo devem estar em consonância com o ordenamento jurídico. Nesse contexto, o papel do Direito é fundamental para garantir a equidade e a transparência nessa relação, bem como a proteção dos interesses públicos e privados envolvidos, que estão, por pressuposto, voltados para a inovação aplicada na área da saúde.

O marco conceitual de inovação (do latim *innovare* ou “fazer algo novo”) teve como seu principal autor o economista Joseph Schumpeter, responsável por introduzir o conceito de ciclos econômicos em consonância ao conceito de inovação. O caráter evolutivo das atividades produtivas, tal qual apresentado pelo economista,

seria o impulso fundamental que inicia e mantém o movimento da máquina capitalista, promovido por novos bens de consumo, métodos de produção ou transporte, mercados e formas de organização industriais criadas pelas empresas (SCHUMPETER, 1961).

As políticas de desenvolvimento produtivo na saúde no Brasil possuem aspectos jurídicos relevantes para serem considerados. Uma das principais questões é a regulamentação por meio da legislação federal, estadual e municipal que garante o direito à saúde. Além disso, existem diversos instrumentos legais que estabelecem as bases para a implementação do Sistema Único de Saúde (sus), assim como os critérios para financiar projetos voltados à produção de medicamentos e dispositivos médicos.

Em primeiro lugar, destaca-se a necessidade da lei federal que garanta direitos fundamentais relacionados à saúde, como assegurado pelo artigo 196 da Constituição Federal. Além disso, há também legislações municipais e estaduais que definem critérios específicos para a implementação de políticas públicas em saúde.

O principal instrumento jurídico utilizado para regular as políticas de desenvolvimento produtivo é a lei de incentivos fiscais, que prevê a concessão de benefícios fiscais para empresas que investem em inovação e tecnologia, bem como que atendem a determinados critérios definidos pelo governo.

Os incentivos fiscais têm como objetivo estimular investimentos em áreas consideradas prioritárias para o desenvolvimento econômico, como as que apresentam grande potencial de geração de emprego e renda (LASTRES; CASSIOLATO, 2011). Entretanto, a concessão de incentivos fiscais deve ser regulamentada por leis específicas e estar sujeita a critérios precisos e transparentes, a fim de evitar abusos e prejuízos aos cofres públicos.

Além dos incentivos fiscais, outras políticas de desenvolvimento produtivo podem incluir a concessão de financiamentos subsidiados, a criação de fundos de investimento, a formação de parcerias público-privadas e a promoção de programas de capacitação técnica e profissional, como será abordado a seguir. Em todos esses casos, o Direito deve estar presente na definição das regras e procedimentos para implementação das políticas, bem como na fiscalização da sua aplicação.

As políticas de desenvolvimento produtivo têm como objetivo promover a competitividade das empresas, a inovação tecnológica, o aumento da produtividade e a melhoria da qualidade dos produtos e serviços. Para isso, são adotadas diversas medidas, sendo que o Direito está presente em todas essas, tais como: incentivos fiscais, investimentos em infraestrutura, políticas de financiamento, ações para o desenvolvimento regional e estímulo ao empreendedorismo.

Os investimentos em infraestrutura, por exemplo, consistem em ações governamentais para a melhoria da infraestrutura, que é fundamental para o desenvolvimento econômico, tais como rodovias, portos, aeroportos, ferrovias, telecomunicações, energia elétrica e saneamento básico (SANTOS; AMARANTE, 2011). Já as políticas de financiamento funcionam como linhas de crédito para financiar projetos de investimentos, com juros mais baixos e prazos mais longos; tais políticas são importantes para que as empresas possam investir em inovação e tecnologia, ampliando assim sua capacidade produtiva.

As ações para o desenvolvimento regional são políticas voltadas para o incentivo do desenvolvimento das regiões com menor desenvolvimento econômico, como a criação de polos tecnológicos e de programas de capacitação. Neste mesmo contexto, há o estímulo ao empreendedorismo por parte do setor público para incentivar a abertura de novas empresas, com medidas como simplificação de processos burocráticos, incentivos fiscais e capacitação empresarial (ROTHWEL, 1984).

Além disso, a regulação do mercado também é um aspecto jurídico importante, uma vez que é responsabilidade do Estado garantir um ambiente de negócios justo e competitivo, bem como proteger os consumidores e incentivar a livre concorrência. Para isso, são criados órgãos reguladores, como a Agência Nacional de Telecomunicações (ANATEL) e a Agência Nacional de Vigilância Sanitária (ANVISA), que têm como objetivo fiscalizar as empresas e proteger os interesses dos consumidores.

Outro ponto importante da análise dos aspectos jurídicos é a Resolução N°39, de 2008, do Ministério da Saúde, que aprova o regulamento para a realização de pesquisa clínica, bem como dispõe sobre o fomento à pesquisa clínica em medicamento humano e equipamento médico no país. O Regulamento para a

obtenção do Comunicado Especial Único para a realização de pesquisa clínica em território nacional é uma norma estabelecida pela Agência Nacional de Vigilância Sanitária (ANVISA), que define as regras e os procedimentos necessários para a realização de pesquisas clínicas em seres humanos no Brasil.

A pesquisa clínica é um estudo científico que envolve a participação de seres humanos, com o objetivo de avaliar a segurança e a eficácia de novos medicamentos, terapias ou procedimentos médicos. Para garantir a segurança dos voluntários e a qualidade dos estudos, a ANVISA estabelece uma série de exigências para a realização de pesquisas clínicas em território nacional.

O Comunicado Especial Único é um documento emitido pela ANVISA, que autoriza a realização de pesquisas clínicas no país. Para obtê-lo, é necessário apresentar uma série de documentos e informações, como o protocolo de pesquisa, a identificação dos pesquisadores responsáveis, a descrição dos procedimentos que serão realizados, entre outros. Além disso, o regulamento estabelece que as pesquisas clínicas devem ser realizadas de acordo com os princípios éticos e científicos estabelecidos pela Declaração de Helsinki e pela Resolução 466/2012 do Conselho Nacional de Saúde, que regulamenta as pesquisas envolvendo seres humanos no Brasil.

Cumprindo salientar, ainda, que a Câmara dos Deputados aprovou o regime de urgência para o Projeto de Lei 7082/17, do Senado, que regulamenta a pesquisa clínica com seres humanos, instituindo o Sistema Nacional de Ética em Pesquisa Clínica com Seres Humanos. O objetivo deste texto é assegurar direitos e princípios éticos na relação entre patrocinador da pesquisa, pesquisador e paciente e, ao mesmo tempo, conferir agilidade na análise e no registro de medicamentos no País.

Por fim, destaca-se também a obrigatoriedade de os fabricantes cumprirem as normas estabelecidas pelo Conselho Nacional de Saúde (CNS) antes do lançamento do produto no mercado nacional. O Conselho Nacional de Saúde (CNS) é um órgão colegiado que tem como objetivo formular e fiscalizar a implementação de políticas públicas de saúde no Brasil. No que se refere ao lançamento de produtos no mercado nacional, o CNS estabelece uma série de normas e regulamentações que devem ser seguidas pelos fabricantes, com o objetivo de garantir a segurança e a qualidade dos produtos.

Antes do lançamento de um produto no mercado nacional, é necessário que o fabricante obtenha a autorização da Agência Nacional de Vigilância Sanitária (ANVISA). Para obter essa autorização, o fabricante deve apresentar uma série de documentos e informações, como o relatório de segurança e eficácia do produto, o plano de monitoramento pós-comercialização, entre outros.

Além disso, o CNS estabelece que todos os produtos devem passar por testes e avaliações rigorosas antes de serem lançados no mercado. Esses testes devem ser realizados de acordo com as normas e diretrizes estabelecidas pela ANVISA e outras agências reguladoras, e devem ser conduzidos por profissionais capacitados e especializados.

O CNS também exige que os fabricantes realizem estudos de segurança e eficácia do produto em diferentes grupos de pacientes, com o objetivo de avaliar a sua segurança e eficácia em diferentes condições clínicas. Em resumo, as normas estabelecidas pelo Conselho Nacional de Saúde (CNS) antes do lançamento do produto no mercado nacional são essenciais para garantir a segurança e a qualidade dos produtos disponíveis para os consumidores brasileiros. Essas normas contribuem para a proteção da saúde pública e para a melhoria da qualidade de vida da população.

3. AS INOVAÇÕES NA SAÚDE

É importante, portanto, a distinção entre invenção, inovação e difusão para o melhor entendimento de suas consequências. A invenção de um novo produto ou processo ocorre dentro da esfera tecno-científica e pode ser sempre mantida com este status. Já a inovação é considerada como um fato econômico e a sua transferência para a esfera tecno-econômica como um evento isolado é decidido majoritariamente pelo mercado. Por sua vez, a difusão, e os sistemas de produção que devem acompanhar determinada inovação, é definida pela extensão da utilização da inovação pelo mercado e pela sociedade e é o que promove efetivamente o crescimento econômico (FREEMAN, 1995).

Uma inovação só terá efeito em larga escala ou duração prolongada se esta for plenamente aceita pelo mercado e pelas pessoas que nele convivem. Em caso de

falha, ela poderá desaparecer por algum período de tempo ou até mesmo indefinidamente. Em caso de sucesso, a inovação poderá ser mantida ainda como um fato isolado ou tornar-se economicamente significativa, a depender do grau de apropriabilidade. Assim, a sua utilização em massa, como um verdadeiro produto competidor ou em outras áreas da atividade econômica, representa o seu grau mais significativo (REINERT, 2004).

3.1 A SAÚDE NO BRASIL

A saúde é um direito fundamental de todo ser humano, conforme estabelecido pela Constituição Federal de 1988. O direito à saúde está diretamente relacionado ao direito à vida e à dignidade humana, pois a saúde é uma condição essencial para o bem-estar físico, mental e social das pessoas. Neste mesmo sentido, a saúde é um fator determinante para o desenvolvimento econômico e social de um país, pois pessoas saudáveis são mais produtivas e têm maior capacidade de contribuir para a sociedade.

Isto significa que todas as pessoas têm direito a um sistema de saúde que garanta o acesso universal e gratuito aos serviços de saúde, independentemente da sua condição social, econômica ou cultural. O Sistema Único de Saúde (SUS) foi criado com o objetivo de garantir o acesso universal e gratuito à saúde no Brasil, por meio de uma rede integrada de serviços de saúde, que inclui desde a atenção básica até serviços de alta complexidade.

No entanto, apesar dos avanços conquistados pelo SUS ao longo dos anos, ainda existem muitos desafios a serem enfrentados para garantir o acesso universal e efetivo aos serviços de saúde. Entre esses desafios, destacam-se a falta de recursos financeiros e humanos, a desigualdade no acesso aos serviços de saúde, a falta de infraestrutura adequada e a baixa qualidade dos serviços oferecidos em algumas regiões do país.

Portanto, a saúde como um direito fundamental deve ser garantida pelo Estado e pela sociedade como um todo, por meio de políticas públicas e ações concretas que visem a promoção, proteção e recuperação da saúde da população. A saúde no Brasil é um tema de grande importância e desafios. Apesar dos avanços nas últimas

décadas, o Brasil ainda enfrenta problemas graves na área de saúde, como a alta incidência de doenças crônicas, como diabetes e hipertensão, a crescente epidemia de obesidade, o aumento de casos de doenças infecciosas, como a dengue e a zika, e a falta de acesso a serviços básicos de saúde em algumas regiões do país.

Ademais, o sistema de saúde do Brasil também enfrenta desafios relacionados à gestão e administração dos recursos, o que muitas vezes resulta em desperdício e má distribuição dos recursos disponíveis. Para enfrentar esses desafios, é necessário investir em políticas públicas que visem a melhoria do sistema de saúde, como a ampliação do acesso aos serviços de saúde, a melhoria da infraestrutura e dos recursos humanos, e a promoção da prevenção e do controle de doenças.

Também é importante destacar a importância da participação da sociedade civil na definição das políticas de saúde e na fiscalização dos serviços oferecidos pelo SUS, a fim de garantir a transparência e a eficácia do sistema. Isto pode ocorrer em diferentes níveis, desde a elaboração e implementação de políticas públicas de saúde até a fiscalização e monitoramento dos serviços de saúde oferecidos pelo Sistema Único de Saúde (SUS); ainda, a sociedade civil também pode participar da definição das políticas de saúde por meio de audiências públicas, consultas populares e outras formas de consulta e engajamento da população.

O setor da saúde no Brasil é responsável por atender às necessidades de saúde da população e garantir que todos tenham acesso aos cuidados médicos. Por isso, é necessário que haja estratégias de promoção de saúde. Algumas das ações de promoção do setor da saúde incluem campanhas de informação sobre doenças, vacinação, acesso a cuidados preventivos e serviços de saúde, além de programas destinados a grupos vulneráveis.

O Ministério da Saúde tem um papel fundamental na execução destas ações. Por meio de seus órgãos e parceiros, o Ministério tem desempenhado um papel essencial na implementação e monitoramento dos programas e iniciativas para promover a saúde da população brasileira. Com isso, é ampliada a garantia de que as políticas de promoção da saúde sejam eficazes e estejam alinhadas com as necessidades da população brasileira. Estas ações são fundamentais para garantir o bem-estar e a qualidade de vida dos brasileiros.

Hodiernamente, o mundo passa por constantes mudanças e desenvolvimento. Com o ritmo acelerado de evolução, vários desafios surgem a cada dia. É necessário que nos adaptemos a essas mudanças e enfrentemos os desafios de forma assertiva para que possamos aproveitar as oportunidades que elas podem nos oferecer. Nessa senda, com o avanço da tecnologia, muitos dos problemas enfrentados podem ser resolvidos mais facilmente. Por exemplo, é possível a utilização de recursos computacionais para processar informações rapidamente, economizando tempo e dinheiro para as empresas. Além disso, esses recursos também podem ser usados para ajudar na tomada de decisões mais acertadas.

No entanto, o maior desafio é o enfrentamento das mudanças no contexto social. É preciso constante adaptação às novas realidades, estabelecendo estratégias de solução de problemas e buscando adotar comportamentos que contribuam para a melhoria da qualidade de vida de todos. Assim, seremos capazes de superar os desafios do presente e futuro.

O setor da saúde brasileiro enfrenta um grande desafio ao tentar implementar políticas de desenvolvimento produtivo que possam melhorar a qualidade dos serviços oferecidos. Apesar dos resultados alcançados até o momento, é importante lembrar que existem muitos desafios a serem enfrentados para promover o crescimento econômico e social do país. É necessário que governos, organizações e empresas trabalhem juntos para superá-los e garantir um futuro melhor para todos os brasileiros.

Portanto, a saúde no Brasil é um tema complexo e desafiador, que exige ações integradas e efetivas para garantir o acesso universal e gratuito aos serviços de saúde, a promoção da prevenção e do controle de doenças e a melhoria da gestão e administração dos recursos disponíveis.

3.2 AS POLÍTICAS DE DESENVOLVIMENTO PRODUTIVO NA SAÚDE NO BRASIL

No Brasil, a saúde é um dos setores de mais destaque na economia e a qualidade dos serviços prestados é decisiva para o desenvolvimento de nosso país. O desenvolvimento produtivo na saúde é uma prioridade estratégica, pois tem o objetivo de garantir a produção de bens e serviços que contribuam para o bem-estar

dos cidadãos. As políticas de desenvolvimento produtivo na saúde buscam promover um ambiente favorável à inovação, à melhoria dos serviços e da qualidade dos produtos oferecidos.

Atualmente, o desenvolvimento produtivo na saúde é um dos assuntos mais importantes para a sociedade brasileira. A saúde é considerada como um direito fundamental e, conseqüentemente, como uma responsabilidade do Estado. Neste cenário, as políticas de desenvolvimento produtivo na saúde no Brasil são essenciais para garantir que os cidadãos tenham acesso a serviços de saúde de qualidade.

Estas políticas buscam promover o desenvolvimento social e econômico da saúde brasileira, melhorando a qualidade dos serviços e garantindo que todos os cidadãos tenham acesso à assistência médica de qualidade. Os objetivos destas políticas incluem o fortalecimento da rede de serviços de saúde, a promoção da inovação tecnológica na saúde e o aumento da participação dos cidadãos na tomada de decisões relacionadas à saúde.

A Política de Desenvolvimento Produtivo na Saúde tem como objetivo promover o acesso universal e equitativo à saúde, garantindo a melhoria da qualidade dos serviços de saúde e a construção de um sistema de saúde mais inclusivo. Esta política é estruturada em quatro diretrizes principais: desenvolvimento institucional, produção e gestão dos serviços, uso racional dos recursos e monitoramento e avaliação.

O desenvolvimento institucional visa aprofundar o compromisso com o Sistema Único de Saúde (sus), fortalecendo as instituições públicas, bem como as organizações da sociedade civil. Além disso, a Política de Desenvolvimento Produtivo procura incentivar a participação da população nos processos decisórios relacionados à saúde.

A produção e gestão dos serviços se concentra no aumento da qualidade dos serviços prestados, melhorando a capacidade diagnóstica, terapêutica e de reabilitação, bem como otimizando os processos de atendimento. O uso racional dos recursos busca garantir o uso adequado dos recursos financeiros e materiais disponíveis para atender às necessidades da população.

Por fim, o monitoramento e a avaliação buscam otimizar o planejamento estratégico do sistema de saúde, assegurando a qualidade do cuidado, bem como

estimulando o aprimoramento contínuo dos serviços oferecidos. A Política de Desenvolvimento Produtivo, no âmbito da saúde, especialmente no caso brasileiro, vislumbra uma saúde mais humanizada, inclusiva e equitativa para todos os brasileiros.

Uma das políticas relevantes surgidas a partir de 2008 no campo do sus foi a Política de Desenvolvimento Produtivo (PDP), derivada justamente da necessidade de se buscar sinergia entre o desenvolvimento industrial tecnológico e produtivo local e a ampliação do acesso da população a medicamentos, vacinas e equipamentos, assim como promover uma melhor alocação de recursos na compra desses produtos. O mecanismo básico posto em prática pela política foi o estímulo à formação de parcerias nas quais uma empresa privada e um laboratório público comprometem-se a entregar em prazo especificado ao Ministério da Saúde um produto identificado por este como estratégico (GUIMARÃES; NORONHA; ELIAS; GADELHA; CARVALHEIRO; RIBEIRO, 2019).

O mecanismo de capacitação tecnológica utilizado nas parcerias era habitualmente o da transferência da tecnologia de um determinado produto do parceiro privado para o laboratório público, o que requer que os laboratórios públicos sejam adequadamente preparados para serem capazes de absorver as tecnologias envolvidas em cada parceria – ressalta-se que grande percentagem dos laboratórios públicos ainda não detêm essa capacidade.

A 2ª Conferência de Ciência, Tecnologia e Inovação em Saúde em 2004 estabeleceu uma estratégia de incorporação de tecnologias no sus como um instrumento de aprimoramento da capacidade regulatória do Estado (REZENDE, 2013). A implantação da estratégia, liderada pelo Ministério da Saúde a partir de 2005, culminou com uma nova política de gestão de tecnologias em saúde, cujo propósito foi o de maximizar os benefícios à saúde garantindo tecnologias efetivas, seguras e em condições de equidade (ALBAREDA; TORRES, 2021).

A nova estratégia foi implementada mediante dois movimentos. Um, direcionado à integralidade da atenção e à institucionalização dos processos de regulação no âmbito governamental, com a criação da Comissão Nacional de Incorporação de Tecnologias no sus (CONITEC), formalizada pela Lei nº 12.401/2011. O outro, voltado para uma política de Avaliação de Tecnologias em Saúde (ATS) com

o objetivo de conferir racionalidade ao processo de incorporação tecnológica. Para isso foi criada, em 2008, a Rede Brasileira Avaliação de Tecnologias em Saúde (REBRATS), envolvendo cooperação do governo com universidades, institutos de ensino e pesquisa, hospitais de ensino e órgãos gestores estaduais e municipais. Sua missão tem sido a de formar massa crítica e disseminar no país a prática de ats (GADELHA; MALDONADO; VARGAS; BARBOSA; SIVEIRA, 2012).

As políticas de desenvolvimento produtivo na área da saúde podem ser uma importante estratégia para o fortalecimento do setor e para a melhoria do acesso da população a serviços de saúde de qualidade. No entanto, é importante ressaltar que a implementação dessas políticas requer uma abordagem cuidadosa e estratégica, levando em consideração as características e necessidades específicas do setor.

Uma das principais vantagens das políticas de desenvolvimento produtivo na área da saúde é que elas podem contribuir para o aumento da produção de equipamentos médicos, medicamentos e outros produtos e serviços relacionados à saúde. Isso pode levar a uma redução dos custos e a uma maior disponibilidade de produtos de qualidade, contribuindo para a melhoria do acesso da população a serviços de saúde.

Além disso, as políticas de desenvolvimento produtivo na área da saúde podem incentivar a inovação tecnológica e a pesquisa e desenvolvimento, o que pode levar a novas descobertas científicas e tecnológicas, além de novos produtos e serviços que possam atender às necessidades da população.

No entanto, é importante ressaltar que a implementação de políticas de desenvolvimento produtivo na área da saúde requer uma abordagem cuidadosa e estratégica, levando em consideração as características do setor e as necessidades da população. É fundamental que essas políticas sejam acompanhadas de medidas para garantir a qualidade e a segurança dos produtos e serviços, além de medidas para garantir o acesso da população aos serviços de saúde.

Em resumo, as políticas de desenvolvimento produtivo na área da saúde podem ser uma importante estratégia para o fortalecimento do setor e para a melhoria do acesso da população a serviços de saúde de qualidade. No entanto, é necessário que essas políticas sejam implementadas de forma cuidadosa e estratégica, levando em consideração as características e necessidades específicas

do setor, e acompanhadas de medidas para garantir a qualidade, a segurança e o acesso da população aos serviços de saúde.

CONCLUSÕES

Verificou-se que a inovação na saúde no Brasil ocorre de forma paulatina, ou seja, de maneira gradual, que é construída em etapas. Muito embora exista uma verdadeira corrida em busca dos avanços que podem beneficiar o maior número de cidadãos no que diz respeito ao desenvolvimento tecnológico aliado à saúde, toda pesquisa é tratada com a cautela necessária, objetivando a garantia da segurança.

A parceria entre os setores público e privado é benéfica no que diz respeito à inovação tecnológica no setor de desenvolvimento de medicações. A Política de Desenvolvimento Produtivo (PDP) vinha enfatizando parcerias envolvendo tecnologias maduras, mas é necessário estender as ações da política não apenas à transferência de tecnologias já dominadas, mas, a encomendas de projetos de desenvolvimento local de tecnologias originais.

As políticas de desenvolvimento produtivo são uma estratégia importante para o crescimento econômico e a geração de empregos em um país. Essas políticas visam incentivar a produção de bens e serviços de maior valor agregado, com o objetivo de aumentar a competitividade e a capacidade de inovação das empresas.

Uma das principais vantagens das políticas de desenvolvimento produtivo é que elas podem contribuir para a diversificação da economia, reduzindo a dependência de setores tradicionais e aumentando a participação de setores de maior valor agregado. Isso pode levar a um aumento da produtividade e da eficiência das empresas, além de gerar novas oportunidades de emprego e renda para a população.

Além disso, as políticas de desenvolvimento produtivo podem incentivar a inovação tecnológica e a pesquisa e desenvolvimento, o que pode levar a novas descobertas científicas e tecnológicas, além de novos produtos e serviços que possam atender às necessidades da população. O incentivo ao desenvolvimento tecnológico é de extrema importância para o progresso econômico, social e científico de um país. Ao incentivar a inovação, a pesquisa e o desenvolvimento de novas

tecnologias, um país pode aumentar sua competitividade, melhorar a qualidade de vida da população e contribuir para a solução de problemas sociais e ambientais.

Em resumo, as políticas de desenvolvimento produtivo podem ser uma estratégia importante para o crescimento econômico e a geração de empregos em um país. No entanto, é necessário que essas políticas sejam implementadas de forma cuidadosa e estratégica, levando em consideração as características e necessidades específicas de cada setor da economia, e acompanhadas de medidas para garantir a sustentabilidade ambiental e social.

As alianças entre as empresas privadas e o Poder Público possibilitam o acesso a muito mais recursos do que qualquer empresa isolada possuiria e por isso inovações de produto e de processo aparecem com maior frequência e com indicadores de qualidade cada vez mais expressivos. A indução de parcerias entre laboratórios farmacêuticos públicos, privados e os produtores de insumos farmacêuticos nacionais configura uma iniciativa induzida pelo governo com o intuito de robustecer o suprimento de produtos para a Saúde. Nessa toada, considera-se atendido o objetivo geral do presente ensaio.

Como consideração final acerca do objetivo específico a que este trabalho se propõe, qual seja, avaliar as parcerias dos setores público e privado para o desenvolvimento tecnológico na saúde do Brasil, foi possível observar que tais parcerias para o desenvolvimento tecnológico na saúde do Brasil têm sido extremamente positivas e têm contribuído para o avanço da pesquisa e desenvolvimento de novos medicamentos e tecnologias na área de saúde. Essas parcerias muitas vezes envolvem colaboração e co-financiamento, o que permite que empresas privadas e instituições públicas trabalhem juntas para desenvolver soluções inovadoras para os desafios do setor de saúde.

Um exemplo de sucesso dessas parcerias é o desenvolvimento de medicamentos no país em caráter de colaboração e financiamento conjunto entre o setor público e privado, que posteriormente são adotados pelo Sistema Único de Saúde (SUS). Esses medicamentos têm sido fundamentais para o tratamento de diversas doenças e para a melhoria da qualidade de vida da população.

Além disso, as parcerias entre os setores público e privado também têm contribuído para o avanço da pesquisa e desenvolvimento de tecnologias inovadoras

na área de diagnóstico e tratamento de doenças, como a telemedicina e a inteligência artificial, que podem melhorar a eficiência e a qualidade dos serviços de saúde.

No entanto, é importante ressaltar que essas parcerias devem ser feitas de forma transparente e ética, garantindo que os interesses da população sejam priorizados em relação aos interesses comerciais das empresas privadas. Também é importante que essas parcerias sejam acompanhadas de medidas para garantir a qualidade e a segurança dos produtos e serviços desenvolvidos, além de medidas para garantir o acesso da população aos serviços de saúde.

Em resumo, as parcerias entre os setores público e privado para o desenvolvimento tecnológico na saúde do Brasil têm sido positivas e têm contribuído para o avanço da pesquisa e desenvolvimento de novos medicamentos e tecnologias na área de saúde. No entanto, é importante que essas parcerias sejam feitas de forma transparente e ética, e acompanhadas de medidas para garantir a qualidade, a segurança e o acesso da população aos serviços de saúde.

REFERÊNCIAS

ALBAREDA, A.; TORRES, R.. Avaliação da economicidade e da vantajosidade nas Parcerias para o Desenvolvimento Produtivo. *Cadernos de Saúde Pública*. 2021.

BRASIL. Constituição Federal (1988). Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm Acesso em: 25 mai. 2023.

BRASIL. Lei nº 10973, de 02 de dezembro de 2004. Dispõe sobre incentivos à inovação e à pesquisa científica e tecnológica no ambiente produtivo e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2004/lei/l10.973.htm Acesso em: 25 mai. 2023.

FARMANGUINHOS; FIOCRUZ. Instituto de Tecnologia em Fármacos/Fundação Oswaldo Cruz. Relatório da Contratação das Parcerias de Desenvolvimento Produtivo (PDP) para a Transferência de Tecnologia de Produção de Medicamentos. Rio de Janeiro. 2011.

FREEMAN, C. The National system of innovation in historical perspective. *Cambridge Journal of Economics*, v. 19, n.1. 1995.

FREEMAN, C.; LOUÇÃ, F. *As time goes by: from the industrial revolutions and to the information revolution*. Oxford: Oxford University, 2001.

GADELHA, C. (Coord). *A dinâmica do sistema produtivo da saúde: inovação e complexo econômico-industrial*. Rio de Janeiro: Editora FIOCRUZ, 2012. Disponível em: <http://books.scielo.org/id/6t3hs/epub/gadelha-9788575415931.epub> Acesso em: 19 nov. 2022.

GUIMARÃES, R.; NORONHA J.; ELIAS, F.; GADELHA, C.; CARVALHEIRO, J.; RIBEIRO, A. Política de Ciência, Tecnologia e Inovação em Saúde. *Ciência e Saúde Coletiva*. 2019. Disponível em: <https://doi.org/10.1590/1413-81232018243.34652018> Acesso em: 25 mai. 2023.

LASTRES, H.; CASSIOLATO, J.; Inovação, arranjos produtivos e sistemas de inovação. In Amaral Filho, J. e Carrillo, J. (coord.) *Trajelórias de Desenvolvimento Local e Regional*, Rio de Janeiro: E-Papers, 2011.

MINISTÉRIO DA SAÚDE. *Resolução N° 39*, de 05 de junho de 2008. Aprova o regulamento para a realização de pesquisa clínica e dá outras disposições. Disponível em: https://bvsms.saude.gov.br/bvs/saudelegis/anvisa/2008/res0039_05_06_2008.htm | Acesso em: 25 mai. 2023.

MINISTÉRIO DA SAÚDE. Secretaria de Ciência, Tecnologia e Insumos Estratégicos. *Análise do Projeto Executivo de Parceria para o Desenvolvimento Produtivo (PDP) de Olanzapina apresentado pelo Núcleo de Pesquisas em Alimentos e Medicamentos - Nuplam*. Nota Técnica nº 122/2012/DECIIS/SCTIE/MS. Brasília. 2012.

NIKOLIC, I.; MAIKISCH, H. Public-Private Partnerships and Collaboration in the Health Sector: An Overview with Case Studies from Recent European Experience. *Health, Nutrition and Population (HNP)*. The World Bank. Washington. p. 1-27, Oct. 2006. Disponível em: <https://openknowledge.worldbank.org/entities/publication/286486ba-11ef-51b9-9aa0-1baf2f32bb37> Acesso em: 25 mai. 2023.

ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD/Eurostat). Oslo Manual. Guidelines For Collecting, Reporting and Using Data on Innovation. 4ª ed. Paris/Eurostat, Luxembourg: *OECD Publishing*. 2018. Disponível em: <https://www.oecd.org/science/oslo-manual-2018-9789264304604-en.htm> Acesso em: 25 mai. 2023.

REINERT, E. *Globalization, Economic Development and Inequality: An alternative Perspective*. Cheltenham: Edward Elgar Pub. 2004.

PRATA, W. *O papel do Sistema Único de Saúde (SUS) na inovação: um estudo sobre transferência de tecnologia no Brasil*. Tese (Doutorado em Medicamentos e Assistência Farmacêutica) – Faculdade de Farmácia, Universidade Federal de Minas Gerais, Belo Horizonte, 2018. Disponível em: <https://repositorio.ufmg.br/handle/1843/BUOS-BB9KAX> Acesso em: 25 mai. 2023.

ROLFSTAM, M. *Public technology procurement as a demand-side innovation policy instrument: an overview of recent literature and events*. Lund: Lund University, 2005. Disponível em <http://www2.druid.dk/conferences/viewpaper.php?id=2553&cf=17> Acesso em: 19 nov. 2022.

ROTHWELL, R. Technology-based small firms and regional innovation potential: the role of public procurement. *Cambridge University Press*, v.4, p. 307-332, 1984. Disponível em: <https://www.jstor.org/stable/3998373> Acesso em: 14 nov. 2022.

REZENDE, K. *As parcerias para o desenvolvimento produtivo e estímulo à inovação em instituições farmacêuticas públicas e privadas*. Dissertação (Mestrado Profissional em Saúde Pública) – Escola Nacional de Saúde Pública Sérgio Arouca (ENSP), Fundação FIOCRUZ, Rio de Janeiro, 2013. Disponível em: <https://goo.gl/5dhhoS> Acesso em: 21 nov. 2022.

SANTOS, N.; AMARANTE, P. (Org.). *Gestão Pública e Relação Público Privado na Saúde*. Rio de Janeiro: Cebes, 2011.

SCHMIDT, F.; ASSIS, L. O Estado como cliente: características das firmas industriais fornecedoras do governo. 17ª edição do boletim Radar: tecnologia, produção e comércio exterior / *Instituto de Pesquisa Econômica Aplicada*. Diretoria de Estudos e Políticas Setoriais, de Inovação, Regulação e Infraestrutura – Brasília: Ipea. 2011. Disponível em: <https://repositorio.ipea.gov.br/handle/11058/5355> Acesso em: 25 mai. 2023.

SCHUMPETER, J. *Capitalismo, Socialismo e Democracia*. Rio de Janeiro: Editora Fundo de Cultura, 1961.

2. OS DESAFIOS ÉTICOS DAS INTELIGÊNCIAS ARTIFICIAIS NA ERA E NO PÓS-ERA DA LEI GERAL DE PROTEÇÃO DE DADOS

*THE ETHICAL CHALLENGES OF ARTIFICIAL INTELLIGENCES IN THE ERA AND
POST-ERA OF THE GENERAL DATA PROTECTION LAW*



<https://doi.org/10.36592/9786554600552-02>

Ana Luiza Liz dos Santos¹

Lucas Moreschi Paulo²

RESUMO

O presente estudo apresenta considerações sobre os desafios de ética, responsabilidade e transparência nas inteligências artificiais a partir das diretrizes da Lei Geral de Proteção de Dados brasileira. O avanço da tecnologia passou a permitir que algoritmos dispensem a ação humana, o que tem potencial para causar prejuízos inimagináveis. O objetivo geral, portanto, é pesquisar de que forma a ética, em sentido amplo, é capaz de evitar e combater discriminações em sistemas de inteligência artificial. Os objetivos específicos alcançam o estudo da ética e da responsabilidade na criação e no treinamento de algoritmos; a análise de como os algoritmos podem recair em decisões discriminatórias e injustas; também a análise

¹ Doutoranda em Direito pela PUCRS. Mestre em Direito pela FMP-RS. Especialista em Proteção de Dados: LGPD e GDPR – Curso Binacional com dupla titulação (FMP-RS e Faculdade de Direito da Universidade de Lisboa). Especialista em Direito Público pela PUCRS. Especialista em Direito Civil e Processo Civil pelo IDC. Graduada em Direito pela PUCRS. Assessora Jurídica no Tribunal de Justiça do Estado do Rio Grande do Sul. Currículo Lattes: <http://lattes.cnpq.br/1213105149446784>. E-mail: analuizaliz.s@hotmail.com.

² Advogado. Doutorando em Direito no Programa de Pós-Graduação em Direito – Mestrado e Doutorado da Universidade de Santa Cruz do Sul (UNISC), bolsista do Programa de Suporte à Pós-Graduação de Instituições Comunitárias de Educação Superior (PROSUC) da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES). Mestre e graduado em Direito pela Fundação Escola Superior do Ministério Público (FMP), foi bolsista institucional do PPGD da FMP. Pesquisador do Grupo de Pesquisa Colisão de Direitos Fundamentais e o Direito como Argumentação, coordenado pelo Prof. Dr. Anizio Pires Gavião Filho, e pesquisador do Grupo de Pesquisa Teoria do Direito: Academia à Prática, coordenado pelo Prof. Dr. Francisco José Borges Motta, ambos do PPGD – Mestrado da FMP e vinculados no CNPq ao Grupo de Estudos Tutelas à Efetivação dos Direitos Transindividuais. Integrante do Grupo de “Pesquisa Jurisdição Constitucional Aberta”, coordenado pela Prof.^a Dr.^a Mônia Clarissa Hennig Leal, vinculado ao PPGD – Mestrado e Doutorado da UNISC financiado pelo CNPq. Membro da *Argumentation Network of the Americas* - ANA. Currículo Lattes: <http://lattes.cnpq.br/4330914363996350>. ORCID: <https://orcid.org/0000-0003-4583-4853>. E-mail: lucasmoreschipaulo@gmail.com.

de como efetivar a transparência e o *accountability* em sistemas de inteligência artificial; e a busca por parâmetros para a construção de uma inteligência artificial mais ética e transparente à luz do que dispõe a Lei Geral de Proteção de Dados brasileira. Conclui-se que a ética e a responsabilidade no design de algoritmos de inteligência artificial são elementos primordiais na realidade de intermediação de ferramentas tecnológicas complexas, inclusive para a sobrevivência da interação entre máquina e sociedade. Para tanto, o estudo foi desenvolvido com base em pesquisa de revisão bibliográfica e legislativa.

Palavras-chave: Algoritmos; Inteligência artificial; Dados pessoais; Ética; Transparência.

ABSTRACT

The present study presents considerations on the challenges of ethics, responsibility, and transparency in artificial intelligence based on the guidelines of the Brazilian General Data Protection Law. Technological advances have made it possible for algorithms to operate without human intervention, which has the potential to cause unimaginable harm. Therefore, the overall objective is to investigate how ethics, in a broad sense, can prevent and combat discrimination in artificial intelligence systems. The specific objectives include studying ethics and responsibility in the creation and training of algorithms, analyzing how algorithms can result in discriminatory and unjust decisions, examining how to achieve transparency and accountability in artificial intelligence systems, and searching for parameters to build a more ethical and transparent artificial intelligence in accordance with the Brazilian General Data Protection Law. The study concludes that ethics and responsibility in the design of artificial intelligence algorithms are fundamental elements in the reality of mediating complex technological tools, including for the survival of the interaction between machines and society. To that end, the study was developed based on a review of literature and legislation.

Keywords: Algorithms; Artificial intelligence; Personal data; Ethics; Transparency.

1. INTRODUÇÃO

Diante do constante processo de amadurecimento das sociedades, o campo do desenvolvimento do ambiente digital, e os seus novos mecanismos, foram sendo criados para suprir o distanciamento dos indivíduos em rede mundial. Na contemporaneidade, o desenvolvimento e o avanço tecnológico são realidades cada dia mais presentes. A Era Digital e a Sociedade da Informação são frutos desse movimento, e protagonizam uma constante reestruturação das relações pessoais, sociais, econômicas, políticas e culturais.

A transformação digital tem como um de seus principais elementos a utilização de inteligência artificial, que é uma realidade que tem, cada vez mais, tomado a atenção do pensamento acadêmico – aí incluído o jurídico – por decorrência da forma que tem afetado a vida em sociedade. Trata-se, em sentido amplo e preliminar, de um conjunto de práticas tecnológicas que se utilizam de dados e algoritmos computacionais, com o objetivo de fornecer resultados inteligentes.

Os assistentes de voz, os corretores automáticos de texto e as ferramentas de identificação facial dos celulares, bem assim os aplicativos de rotas com previsão de chegada e algoritmos de redes sociais, são apenas alguns exemplos de inteligência artificial que são usadas rotineiramente, diversas vezes ao dia, por milhares de pessoas. Isso significa dizer que, em que pese para muitos a inteligência artificial seja “coisa do futuro”, em verdade, está presente na vida de muitas pessoas, mesmo sem o conhecimento específico acerca da correlação entre mecanismo e nomenclatura.

De mais a mais, tem-se que, dos mais simples aos mais complexos, praticamente todos os programas de computador se utilizam de algoritmos, que representam uma sequência de instruções que têm por objetivo o processamento de informações para uma finalidade específica. A partir da formação de estereótipos, contudo, não raras vezes os algoritmos recaem em decisões de caráter discriminatório e injusto, o que merece ser combatido, inclusive e especialmente para assegurar a proteção dos direitos fundamentais.

Desta realidade decorre a relevância de se combater a opacidade dos algoritmos, uma vez que a compreensão e a avaliação das decisões tomadas são

primordiais para a garantia da transparência e do *accountability* e, por consequência, para a garantia do uso adequado das ferramentas de automação decisória.

No Brasil, à exemplo da tendência mundial, a resposta dada para o novo influxo do compartilhamento de dados pessoais foi a edição da Lei Geral de Proteção de Dados (LGPD). Quase cinco anos após a sua promulgação, porém, o foco parece estar mais em torno dos processos que se relacionam com o gerenciamento dos riscos que decorrem das atividades dos programas inteligentes no tratamento de dados pessoais, do que propriamente na perspectiva da autodeterminação informativa.

Por estas considerações, com base em pesquisa de revisão bibliográfica, o presente estudo se propõe, em um primeiro momento, a analisar a essencialidade da ética e da responsabilidade na criação e no treinamento de algoritmos, com vistas à garantia dos pilares da vida em sociedade. Em seguida, pretende estudar como o algoritmo pode recair em decisões discriminatórias e injustas, a partir do que é conhecido por viés algorítmico. Na sequência, objetiva adentrar no estudo da transparência e do *accountability* em sistemas de Inteligência Artificial, como formas de evitar e de combater os movimentos discriminatórios. Finalmente, busca apresentar parâmetros para a construção de uma Inteligência Artificial mais ética e transparente, especificamente à luz da Lei Geral de Proteção de Dados brasileira.

2. ÉTICA E RESPONSABILIDADE NA CRIAÇÃO E NO TREINAMENTO DE ALGORITMOS

Não há ainda um consenso sobre o que é ética na implementação, treinamento e uso das inteligências artificiais, e menos ainda há uma noção bem estruturada sobre a ética das inteligências artificiais (IAs). Ainda assim, há claras preocupações centrais dentro das reflexões sobre a filosofia ética que devem ser estruturalmente alocadas de forma adequada para dentro do universo de funcionamento das IAs. Nesse sentido, é importante trazer à conhecimento aspectos deontológicos que estruturam a base na qual tanto eventual e futura regulação, ou ação do poder judiciário para a tutela de direitos em situação de tutela requerida em face ou a partir da utilização de IAs.

Nesse sentido, importante ressaltar que a ética necessária nas IAs vai muito além do uso adequado, plural e consciente das bases de dados e métodos de treinamento dos algoritmos. Passa, sobretudo, pelo endereçamento adequado dos contornos éticos que devem existir para serem exigidos futuramente em situações de necessidade para seu controle (VAKKURI; ABRAHAMSSON, 2018). Pondo em melhores termos, a ética nas e das IAs deve ser vista como regra, aplicável sempre e indistintamente em sua máxima, ou como princípio, sendo aplicável na melhor medida adequada possível tendo em mente fins e possibilidades *in casu* de sua aplicação e exigência ética?

O que se deve assinalar, então, é que o cuidado para com os planos metafísicos, teóricos, filosóficos e jurídicos que estão associados na relação entre Inteligência Artificial e Direito sirvam como motriz para compensar o rápido avanço e o constante incremento da implementação da IA no cotidiano das vidas civis. A capacidade de processamento cada vez mais acentuada e dinâmica, todo dia mais potente, deve abrir espaço epistêmico e existencial para abraçar também uma dimensão ética de respeito às dimensões humanas e aos seres humanos, bem como uma relação de tutela e zelo aos direitos fundamentais, sobretudo quando a aplicação de IA tenha impacto direto e imediato sobre a vida, e nesse quesito na fruição de direitos, dos indivíduos (YAPO; WEISS, 2018, p. 5368).

É crucial que se leve em conta não apenas os resultados imediatos produzidos pela tecnologia da IA, mas também os efeitos secundários que podem atingir os indivíduos envolvidos e as esferas sociais mais amplas. Além disso, é preciso adotar uma abordagem ampla e integrada para lidar com as oportunidades e os riscos ligados à IA, a fim de assegurar que os direitos fundamentais e a ética sejam protegidos e respeitados em todas as áreas da sociedade em que a IA é implementada. Uma preocupação central em termos de ética e tutela de direitos está no viés algorítmico, que ocorre quando os algoritmos utilizados para tomar decisões e realizar tarefas incorporam preconceitos e desigualdades existentes na sociedade a partir de sua base de dados. Isso pode levar a resultados discriminatórios, de modo que é especialmente importante que os desenvolvedores de algoritmos levem em consideração a diversidade e a inclusão em todo o processo de criação e

implementação da IA, a fim de garantir que os algoritmos sejam justos e não perpetuem injustiças existentes na sociedade.

Os efeitos associados às possibilidades de uso de algoritmos complexos, com impacto nas mais variadas áreas da sociedade, são de extrema importância. Hoffmann-Riem (2019, p. 14) ensina que é preciso conceber um enfoque amplo à forma de lidar com as oportunidades e os riscos ligados à inteligência artificial e, precisamente, ao seu emprego, não devendo, para tal, o foco restringir-se aos resultados produzidos diretamente com a tecnologia digital mediante uso de inteligência artificial. São igualmente importantes os efeitos que alcançam os destinatários de decisões ou terceiros atingidos, bem assim os efeitos adicionais, inclusive a longo prazo, nas esferas da sociedade.

Considerados os riscos de uso de algoritmos decisórios é possível pensar, para além do arcabouço normativo já existente, em três importantes pilares que devem nortear a criação e o treinamento de algoritmos: princípio da auditabilidade, princípio da transparência e princípio da consistência ou regularidade procedimental (LORDELO, 2021, p. 234). A auditabilidade representa o registro das informações, a transparência impõe que as informações possam ser de forma adequada acessadas e explicadas, e a consistência representa a paridade de procedimentos para os destinatários de uma ferramenta construída por algoritmos.

Além disso, é importante ressaltar que a análise de dados deve ser feita levando em conta os 5 Vs dos dados: volume, velocidade, variedade, veracidade e valor, como aponta Laney (2001). O volume diz respeito à quantidade de dados disponíveis, a velocidade se refere à rapidez com que esses dados são gerados e processados, a variedade inclui a diversidade de tipos e formatos de dados, a veracidade está relacionada à confiabilidade e precisão dos dados e o valor está ligado à utilidade e relevância dos dados para as tomadas de decisão. Levar em consideração esses cinco fatores é essencial para garantir que os dados sejam coletados, processados e utilizados de maneira responsável e ética, evitando possíveis efeitos negativos para a sociedade.

Fato é que a noção de uma inteligência artificial ética deve ser abarcada por todas as partes interessadas, com soluções dotadas de integridade e/ou precisão em relação ao seu propósito, uma vez que a máquina aprende com base nos dados

que processa, os quais, se não forem representativos ou precisos, acabarão desenvolvendo resultados potencialmente antiéticos (PASETTI, 2023, p. 175). Importante, ainda, para uma inteligência artificial ética, que os valores e princípios orientadores sejam aplicados às tecnologias, sendo incorporados, destaca-se, desde a sua concepção, como um padrão em todo o ciclo de vida da inteligência artificial (PASETTI, 2023, p. 178).

Dentre as muitas questões éticas, destacam-se a relacionada ao princípio da autonomia, a partir da verificação do ponto máximo em que uma máquina detém independência para tomar decisões, bem assim a relacionada à identificação da responsabilidade pelas ações induzidas pelos algoritmos (ROSSETTI; ANGELUCI, 2021, p. 4-5). Isso porque a capacidade de aprendizado confere aos algoritmos certo grau de autonomia, de modo que a ação humana, que até determinado momento era necessária para a programação de algoritmos e sistemas algorítmicos complexos, passou a se tornar menos importante nos sistemas de aprendizagem, o que tem por consequência uma possível falta de controle humano no desenvolvimento futuro autogerido de programas (HOFFMANN-RIEM, 2020, p. 15-16). Nesse cenário, os programadores podem perder a transparência e a rastreabilidade dos processos, o que, em contrapartida, sustenta os alertas acerca do uso ilimitado da inteligência artificial.

A ética e a responsabilidade na criação e no treinamento de algoritmos, pois, figuram como essenciais inclusive para a sobrevivência da sociedade. Como bem dispõe Harari (2023), o tamanho e o montante de benefícios da inteligência artificial não importam se a sua base ruir. Por isso, é imprescindível que sejam considerados os riscos associados ao viés algorítmico e à discriminação na tomada de decisões, a fim de garantir que a IA seja utilizada de maneira justa e equitativa em todas as esferas da sociedade. O viés algorítmico também está presente nos resultados das decisões automatizadas, e sua discriminação resultante do enviesamento pode prejudicar grupos já marginalizados. Dessa forma, é fundamental que os desenvolvedores de algoritmos trabalhem para identificar e mitigar o viés algorítmico em todo o processo de criação e treinamento dos algoritmos, adotando práticas éticas e responsáveis para garantir que a IA seja uma força positiva para a sociedade como um todo.

3. VIÉS ALGORÍTMICO E DISCRIMINAÇÃO NA TOMADA DE DECISÕES

Algoritmos são um conjunto de instruções lógicas que um programa de computador segue para concluir uma tarefa específica em uma sequência escalonada de passos. Eles são modelos sistemáticos de comandos, que fornecem uma sequência organizada de etapas para alcançar um resultado desejado. Os algoritmos são empregados em quase todos os programas de computador, desde os mais simples, como um editor de texto, até os mais sofisticados, como um software de inteligência artificial estrita (*narrow artificial intelligence*), que utiliza técnicas de aprendizado de máquina (*machine learning*) para treinar algoritmos a realizar tarefas específicas sem ter que serem programados para executá-las rigidamente.

Atualmente, os algoritmos são utilizados em diversos setores, apresentando vantagens e desvantagens para atividades que antes eram executadas somente por seres humanos. Alguns exemplos incluem a otimização de processos burocráticos em plantas industriais, tomada de decisões no mercado financeiro, na agricultura, meio ambiente e fornecimento de serviços básicos, como água e energia elétrica, entre muitos outros. No entanto, é cada vez mais evidente que esses algoritmos podem ser afetados por preconceitos e estereótipos presentes em nossa sociedade, resultando em um fenômeno conhecido como viés algorítmico.

A ocorrência de viés algorítmico pode levar a decisões discriminatórias e injustas, o que é particularmente preocupante em áreas como a justiça criminal, seleção de candidatos a empregos e concessão de crédito. Portanto, é fundamental garantir que a utilização da Inteligência Artificial esteja em conformidade com os princípios éticos e constitucionais para evitar a produção de resultados que prejudiquem a fruição de direitos fundamentais, de forma intencional ou não, especialmente em decisões importantes para o cotidiano das vidas individuais. É, portanto, essencial abordar o enviesamento algorítmico e buscar entender como podemos equacioná-lo dentro da lógica das Inteligências Artificiais (IAs), para que as decisões tomadas por elas ou com seu auxílio sejam justas, éticas e respaldadas pela Constituição.

Os dados são uma fonte de poder extremamente forte e superior ao petróleo. O valor do petróleo está intrinsecamente ligado à sua disponibilidade, visto que é um

recurso finito e de extração complexa. Já os dados estão disponíveis em grande quantidade e são infinitos, e enquanto a humanidade existir, haverá consumo, economia e, conseqüentemente, geração de dados. Por trás de tudo isso, estão as decisões automatizadas, alimentadas pelos dados, que são seu combustível. O valor de um bem intangível não pode ser adequadamente compreendido apenas pelo paradigma mercadológico tradicional. A valorização do conhecimento e o direcionamento que as grandes empresas podem obter a partir dos dados só é possível na nova concepção de economia digital, que acontece através da rede.

Com a capacidade de utilização dos dados para o *profiling*, análise comportamental de mercado e ofertas de marketing direcionadas, se foi capaz pela primeira vez de promover uma verdadeira revolução: transformou o consumidor em produto e os fornecedores em consumidores de dados. O consumidor deixou de ser o fim da linha mercadológica e tornou-se o centro da cadeia produtiva.

De fato, a discriminação algorítmica é uma questão preocupante e que merece atenção por parte dos desenvolvedores de tecnologias e dos legisladores. Um exemplo emblemático é o COMPAS (Correctional Offender Management Profiling for Alternative Sanctions), um sistema utilizado em alguns estados dos Estados Unidos para prever a probabilidade de um indivíduo cometer crimes no futuro, com base em uma série de fatores, como histórico criminal e dados socioeconômicos. O problema é que estudos mostram que o COMPAS é tendencioso, com uma taxa mais alta de falsos positivos para pessoas negras e latinas, em comparação com pessoas brancas. Isso significa que, muitas vezes, pessoas inocentes são consideradas como tendo uma alta probabilidade de cometer crimes futuros, apenas por causa da sua raça ou etnia.

Esse exemplo ilustra como a discriminação algorítmica pode ter conseqüências graves na vida das pessoas, especialmente quando se trata de decisões que afetam sua liberdade e segurança. É preciso, portanto, desenvolver sistemas mais justos e transparentes, que levem em conta a diversidade e a complexidade da sociedade, sem perpetuar preconceitos e estereótipos. Do contrário, se está diante de uma discriminação algorítmica, ou, ainda, de viés algorítmico (PARANHOS, 2022, p. 7).

Uma experiência central para compreender o malefício deste viés é o caso do algoritmo COMPAS, que nada mais é do que uma ferramenta de perfilização de gerenciamento corretivo de infratores para sanções alternativas que indica o índice de reincidência dos acusados e cujos resultados (que são discriminatório) não impugnáveis, pois tomados por máquinas de baixa sindicabilidade. Com o passar do tempo o COMPAS dava como resposta que pessoas negras eram de alto risco e as pessoas brancas como de baixo risco, e o fazia a partir do cruzamento de informações da sua base de dados. O'Neil (2020, p. 42-43) descreve cenário do COMPAS, a partir de uma base de dados formada a partir das respostas de detentos a questionários LSI-R, que era um questionário cujas respostas entregariam, por si, a medida estatisticamente comprovada da chance de um detento reincidir na lida delituosa. A partir desse questionário foi montado um sistema de respostas altamente correlacionados em que a similitude entre uma pessoa presa pela primeira vez e um detento já reincidente faziam com que o score subisse, isto é, a chance de que cometeria crimes novamente. Para tanto, de maneira antijurídica, eram avaliados dados sensíveis como nome da família, bairro em que nasceu e cresceu, se amigos já foram presos, as circunstâncias do nascimento, etc.

O sistema montado a partir do LSI-R até pode ser muito efetivo para medir estatisticamente o risco de reincidência. Contudo, não poderia ser utilizado por ofensa à presunção da inocência (no segundo crime hipotético) e a imparcialidade, bem como não poderia guiar de maneira isolada um aumento de pena ou restrição corporal em regime mais gravoso. Essas são algumas implicações centrais do (mal) uso dos algoritmos na atual conjuntura da vida, que passa desde bonequinhos e avatares na internet, como se verá, até questões centrais dos sistemas de acessos a direitos.

Algoritmos tem potencial discriminatório simplesmente por utilizar dados. Se os dados históricos forem prejudiciais ou não representativos da população, os algoritmos podem refletir esses dados e perpetuar padrões não desejáveis. O problema é que não há inteligência artificial, nem algoritmos, nem ferramentas automáticas para auxiliar o ser humano, sem o uso de dados. A qualidade da inteligência e do processamento de dados depende diretamente do volume e da qualidade dos dados. Fatalmente, os algoritmos acabam discriminando pessoas

com base em vieses herdados ou não identificados por sua base de dados ou por seus programadores. Características como gênero, raça e classe social facilmente servem para classificar pessoas, e isso tem especial potencial lesivo dentro da linguagem de máquina. Os algoritmos podem usar estas características para determinar se uma pessoa será contratada, se receberá um empréstimo ou se será admitida em uma universidade, de modo automático, frio e calculista. Isso não parece desejável para um mundo civilizado e uma sociedade madura em termos de direitos humanos e fundamentais.

O'Neil (2020, p. 13), alerta sobre os riscos da discriminação algorítmica, tendo em vista a constatação de que ao algoritmos podem perpetuar preconceitos e estereótipos, levando a decisões injustas e desiguais, afetando negativamente pessoas de grupos minoritários, como mulheres, negros, latinos e LGBTQs, e ainda mais pessoas que são diversamente discriminada, isto é, por mais de uma característica. Isso se dá pela falta de freios éticos dentro das linhas da programação das inteligências artificiais, isto é, de seus algoritmos. É o prisma da interpretação sobre os dados que conforme, em muito, o resultado do algoritmo. Quanto menor for sua programação para que combata ativamente a discriminação algorítmica, maior será a probabilidade de que venha a entregar um resultado discriminante.

Uma das principais preocupações ético-jurídicas em relação à discriminação algorítmica é exatamente a transparência do código-fonte dos algoritmos e da base de dados que o supre (BUITEN, 2019, p. 44). Como os algoritmos são muitas vezes considerados caixas-pretas, é difícil saber como as decisões são tomadas e se elas são justas e imparciais. Isso pode violar princípios fundamentais do direito, como o devido processo legal e a igualdade perante a lei.

Para que se possa garantir decisões de base algorítmica mais justas, imparciais e menos discriminatórias é necessário que se cuide com **i)** a qualidade dos dados utilizados pelos algoritmos, isto é, os dados devem ser verdadeiros, precisos, relevantes, imparciais e diversificados, eles devem refletir a diversidade da sociedade e não podem permitir a perpetuação de preconceitos ou estereótipos. Uma boa decisão automatizada começa com uma boa base qualitativa de dados.

Um segundo cuidado a se ter é o da **ii)** transparência do funcionamento dos algoritmos, algo que ainda é uma caixa-preta regulatória, jurídica e de programação,

uma vez que o funcionamento dos algoritmos é protegido pela propriedade intelectual da empresa desenvolvedora. Exige-se, nesse ponto, um necessário novo olhar a partir da colisão existente entre o direito à propriedade intelectual e o segredo de fábrica, de um lado, e o direito à transparência algorítmica, à fundamentação algorítmica e à não discriminação – quando essa for ocasionada diretamente pela ausência de clareza de sua programação e de sua base de dados.

Outro ponto crucial a se alinhar é **iii)** o cuidado com a ética e a responsabilidade social das empresas de desenvolvimento para com o resultado de seus produtos. Ter práticas de ESG (*environmental, social and Governance*), p.e., podem vir a ter um papel importante nos rumos do desenvolvimento da programação e dos algoritmos, ao se trazer maior diversidade às equipes de programação, comungando e somando experiências sociais e geográficas de diferentes origens e perspectivas, levando em consideração a maior soma possível da diversidade existente na sociedade.

Os três pontos sinalizados supra comungam para a necessidade da regulamentação do desenvolvimento e do uso dos algoritmos, em processos que sejam auditáveis, transparentes e que tenham o condão de promover o direito à não discriminação algorítmica, dentre outros também amealhados. Deverá ser encontrado um equilíbrio entre a valorização dos avanços tecnológicos e das inovações pelas empresas, resguardando seus interesses comerciais, ao mesmo tempo em que se tenha a valorização do ser humano, não enquanto um fornecedor (semi-inconsciente) de dados, mas enquanto utilizador e consumidor final dos algoritmos. O ser deve ser tratado como um fim em si, e não como um meio para o melhoramento da máquina.

Dessa forma, como se viu, a discriminação algorítmica é uma preocupação jurídica atual e que seguirá para o futuro próximo. Algoritmos e inteligências artificiais tem especial facilidade em se tornar relevantes e integrados na vida humana do cotidiano. O fato de que podem perpetuar preconceitos e estereótipos, levando a decisões injustas e desiguais é fato relevante o suficiente para que o embate jurídico e o combate à discriminação esteja autorizado a existir. Além disso, é importante garantir a qualidade dos dados, a transparência dos algoritmos, a diversidade nas equipes de desenvolvimento, a responsabilidade das empresas para

que se chegue a uma fórmula de regulamentação e de regulação adequada à (nova) realidade promovida pelos algoritmos.

4. TRANSPARÊNCIA E *ACCOUNTABILITY* EM SISTEMAS DE INTELIGÊNCIA ARTIFICIAL

A transparência algorítmica é fundamental para garantir o uso adequado das ferramentas de automação decisória. A opacidade dos algoritmos pode dificultar a compreensão e avaliação das decisões tomadas, o que pode afetar a transparência e *accountability* do sistema judiciário. Além disso, a utilização de dados históricos que refletem preconceitos sociais pode levar à discriminação algorítmica. Nesse sentido, é importante compreender os desafios envolvidos na promoção da transparência algorítmica, como uma dimensão instrumental apta a promover o desenvolvimento da tomada de decisão por algoritmos.

A tomada de decisão apoiada com base em algoritmos pode parecer objetiva, mas na verdade estão carregadas de dados e do seu natural ou não-natural enviesamento, o que fatalmente leva, em um grande número de casos, a resultados injustos, como a recusa de emprego ou a negação de crédito por motivos como raça, sexualidade, origem, ou ainda, como é mais comum, ser eliminado de processo seletivo de emprego pelo fato de ter atrasado o pagamento de contas em um mês – o que poderia demonstrar desleixo. Ainda que tais considerações possam ser fundamentadas e comprovadas empiricamente e cientificamente, não podem servir de motivos para a tomada de decisão, visto que ofendem a dignidade da pessoa humana.

A transparência e o *accountability* são aspectos fundamentais para garantir a confiança e a legitimidade dos sistemas de inteligência artificial (IA) e, conseqüentemente, a proteção dos direitos e das liberdades individuais dos usuários. A análise de como efetivar a transparência e o *accountability* em sistemas de IA, portanto, é crucial para o desenvolvimento de políticas e normas que regulem o uso dessa tecnologia, tanto e, âmbito público quanto em âmbito privado.

Pasquale (2015), explora como as empresas e os governos já utilizam há anos algoritmos para tomar decisões centrais e cruciais, como política monetária ou investimentos. Pasquale (2015, p. 160) argumenta que tais práticas podem até

ocorrer, mas não podem ser uma caixa-preta – daí o título de seu livro – visto que necessariamente devem ter mais transparência e responsabilidade, sobretudo quando o resultado decisório atinge diretamente o ser humano.

A necessidade de transparência, em especial, tem o condão de imediatamente coibir certas práticas corporativas e governamentais que direcionam programações discriminatórias – o uso de programas discriminatórios pode vir a configurar o crime de racismo, por exemplo – e sob uma perspectiva mediata, a transparência tem o condão de abrir a caixa-preta dos algoritmos e permitir um ajuste mais fino e sofisticado nas ferramentas, entregando respostas cada vez mais coerentes para com o núcleo do Estado Democrático de Direito, que atualmente vem sendo ofendido.

Um dos principais desafios para efetivar a transparência em sistemas de IA é a falta de clareza sobre como as decisões são tomadas, isto é, quais são os processos e caminhos lógicos de 1 e 0, sim e não, que os algoritmos empregam em cada etapa, e como cada etapa, e cada dado, contribuem para a resposta final. Isso é a *black box* de Pasquale (2015). Assim, não é possível entender como uma determinada decisão foi tomada, mesmo que seus resultados possam ser avaliados, visto que a “racionalidade da decisão” é um mistério. Uma forma de solucionar esse problema é por meio do desenvolvimento de modelos explicáveis de IA, que permitam aos usuários entender como os resultados foram obtidos. Além disso, a divulgação das informações sobre o treinamento dos algoritmos e os dados utilizados também é essencial para garantir a transparência.

A essencialidade da promoção de um elevado grau de transparência algorítmica, de modo a possibilitar o conhecimento daquilo que determina o resultado pela ferramenta, é substancial (LORDELO, 2020, p. 149). Isso é alcançado sobremaneira a partir do convite à inclusão de preocupações éticas que, somadas as apresentadas acima, ainda devem contar com etapas de verificação, validação, segurança e controle (PEIXOTO; SILVA, 2019, p. 37-39). A verificação diz respeito à aferição da confiabilidade do sistema para o tratamento e construção de situações críticas de segurança. Isso tem especial importância no que diz respeito com a demanda ética, que se transparece sempre que demandado ou exigido por critérios de segurança no tratamento e uso de dados ou nos procedimentos matemáticos e

de programação que restringem ou possibilitam a distância e o alcance das aplicações de IA.

Já a etapa de validação diz respeito à confirmação de que o sistema foi projetado, construído e executado de maneira a atender um bom comportamento sob o ponto de vista técnico e ético. Isto é dizer que, além da confiabilidade técnica na execução de maneira ética, há eficácia no uso que se pretende fazer. No caso de um carro autônomo, que deve tomar decisões a todo instante, como a mera decisão de continuar dirigindo mantendo a velocidade, essa etapa de validação é a etapa que comporta a confirmação de que o automóvel autônomo executa de maneira correta, sob ponto de vista técnico, e de maneira adequada, sob ponto de vista ético. Ele tanto dirige tomando as melhores decisões, como ele não irá escolher atropelar uma pedestre para desviar de uma árvore; irá, idealmente, frear.

A etapa de segurança, ou da verificação da segurança, é aquela que diz respeito à verificação das etapas de segurança das inovações da aplicação (sempre que ocorrerem), evitando-se que a IA caia em um mau uso como, por exemplo, a sua ocupação por *hackers* ou então seu encaminhamento nocivo por usuários. Há, portanto, uma possibilidade de enviesar defensivamente a IA, de modo que ela evite, a partir de limitadores éticos programados, o cometimento de crimes, ou seu auxílio. A segurança está diretamente relacionada com a redução das vulnerabilidades.

Por fim quanto essas etapas, a etapa de controle é aquela que, dentre todas, ganha especial relevância. A etapa de controle é aquela que identifica certos *stops* estratégicos, etapas nos quais a máquina não pode avançar sem que um controlador humano dê permissão. Esse resguardo de programação para com o envolvimento da ética humana na programação de máquinas, e mesmo no *machine learning* é central para as políticas de ética e privacidade *by design*. Aqui se identifica, por exemplo, uma forma de que quando a máquina notar que potencial resultado é discriminatório, ela acione o humano para questioná-lo sobre a ética de tal decisão automatizada. Muito importante para tanto é o uso adequado do *feedback*, ferramenta com a qual a máquina pode entender a adequação ou não de sua resposta, reforçando as boas respostas e descartando as respostas indesejáveis (O'NEIL, 2020, p. 207).

Nessa última etapa há o destaque entre o que a máquina pode fazer por si só e o que um controlador humano necessariamente deve fazer por ela. A arquitetura

dos protocolos não é o centro da ausência de luz, a opacidade está nos pormenores das múltiplas engrenagens que ficam atrás das paredes da sala algorítmica (POLONSKI, 2018). Por isso que o grau de satisfatoriedade nestas dimensões parafuncionais dos algoritmos é tão dependente do mesmo fator de seu sucesso estrito: a habilidosa capacidade do programador humano em construir e fortificar um algoritmo capaz de entregar o melhor resultado deixando mais visíveis os rastros lógicos de sua funcionalidade (STEINER, 2012). Há, no entanto, outro fator a ser avaliado, mas em pesquisa dedicada a tanto: o segredo comercial em colisão com o direito à transparência algorítmica e à explicabilidade.

Dando sequência, é importante ressaltar que a opacidade dos algoritmos pode dificultar a identificação e correção de possíveis erros ou vieses. A aplicação de algoritmos pode ser afetada por problemas em diversas etapas, sendo que a definição das regras e o uso de dados inadequados são especialmente suscetíveis a gerar questões. Diante disso, há uma preocupação crescente com três grandes problemas que podem surgir em decorrência do uso de algoritmos. O primeiro é o uso de conjuntos de dados enviesados, que podem levar a resultados equivocados e injustos. O segundo é a falta de transparência em algoritmos não programados, que torna difícil entender como as decisões são tomadas e contestá-las quando necessário. O terceiro problema é a possibilidade de discriminação que pode ser gerada por algoritmos de aprendizado de máquina. Por isso, é importante estar atento a esses problemas ao utilizar algoritmos em diferentes contextos (FERRARI; BECKER; WOLKART, 2018, n.p.).

A importância da transparência algorítmica se dá para garantir o uso adequado das ferramentas de automação decisória. A transparência algorítmica possibilita o conhecimento daquilo que determina o resultado pela ferramenta, evitando riscos como discriminação algorítmica e garantindo a responsabilização dos agentes envolvidos no processo decisório.

A efetivação do *accountability* em sistemas de IA é um desafio grande, uma vez que muitas vezes não há uma clara responsabilidade sobre as decisões tomadas pelos algoritmos e, na atual quadra histórica da relação Direito e IA, ainda não há qualquer segurança sobre qual o papel do produtor, do comerciante, do atirador, da munição e da arma, em um homicídio, sabe-se apenas que a arma é poderosa e que

seus resultados são tanto construtivos quanto destrutivos. Algoritmos são, nessa toada, tão poderosos quanto as habilidades de seu programador e de seu utilizador, e tão nocivos quanto a maldade ou a indiferença destes mesmos atores. O algoritmo sozinho, no entanto, não tem (espera-se) vontade própria. Isso ocorre porque os sistemas de IA são frequentemente projetados para operar de forma autônoma, sem intervenção humana direta e a partir de estruturas lógicas encabeçadas e repetitivas (padronizadas). Nesse sentido, uma forma de garantir a responsabilidade é por meio do desenvolvimento de sistemas de governança que estabeleçam claramente as responsabilidades dos diferentes agentes envolvidos na cadeia de produção e uso da IA (REIS, 2020, p. 161-168).

Em conclusão, a transparência algorítmica é fundamental para garantir o uso adequado das ferramentas de automação decisória. A opacidade dos algoritmos pode dificultar a compreensão e avaliação das decisões tomadas, afetando a transparência e *accountability* do sistema judiciário. Para evitar riscos como discriminação algorítmica e garantir a responsabilização dos agentes envolvidos no processo decisório, é essencial promover um elevado grau de transparência algorítmica. Isso significa possibilitar o conhecimento daquilo que determina o resultado pela ferramenta, evitando riscos como discriminação algorítmica e garantindo a responsabilização dos agentes envolvidos no processo decisório.

5. A LEI GERAL DE PROTEÇÃO DE DADOS E A CONSTRUÇÃO DE UMA INTELIGÊNCIA ARTIFICIAL MAIS ÉTICA E TRANSPARENTE

A Lei Geral de Proteção de Dados brasileira (LGPD) representa um marco histórico – não apenas legislativo, mas de caráter geral no ordenamento jurídico pátrio – para a tutela dos dados pessoais em nosso país. Após diversas tentativas frustradas, às quais pode ser atribuído, inclusive, falta de interesse, foi apenas no ano de 2018, com a Lei nº 13.709, que o Brasil adentrou no rol de países com legislação específica sobre a temática.

Em verdade, para além da sua formalidade normativa, que é importante, mas não suficiente, a LGPD inaugurou uma base específica para que valores e princípios já existentes em nosso ordenamento jurídico fossem orientados em torno de uma

disciplina de caráter geral, a partir de uma noção uniforme e padronizada no encaminhamento das diversas situações que decorrem do tratamento de dados pessoais (DONEDA, 2020, p. 245). Mais ainda porque trata-se de uma Lei com perfil de código, ou microssistema, dotada de regras e procedimentos, os quais devem estar presentes em qualquer instituição, pública ou privada, que promova o tratamento de dados pessoais, inclusive no ambiente digital (NEGRÃO, 2020, p. 30).

A compreensão sobre o papel e o alcance da Lei Geral de Proteção de Dados, por sua vez, representa um dos principais desafios postos a partir da promulgação e da entrada em vigor do texto, tendo em vista que são diversos os fatores, todos dotados de relevância, que são afetados pelas disposições legislativas. Ademais disso, configura-se como primordial um necessário enfoque material a ser conferido à Lei, com vias a assegurar os direitos por ela formalmente e materialmente tutelados.

O direito fundamental à proteção de dados pessoais, principal ponto de atenção da legislação específica e assim reconhecido de forma expressa no Brasil a partir da Emenda Constitucional nº 115/2022³, tem, por sua vez, a inteligência artificial como um de seus mais importantes desafios da atualidade contemporânea e possivelmente do futuro. Isso porque a inteligência artificial, programada por algoritmos, tem como uma de suas principais matérias-primas justamente os dados pessoais.

Em assim sendo, e uma vez que, no contexto da Sociedade da Informação e da Era Digital, não existem dados pessoais que possam ser considerados insignificantes, na medida em que os dados que em uma determinada circunstância podem não acarretar riscos ou danos, em algum momento futuro, e/ou a partir da combinação com outros dados, podem o ser, tem-se que a articulação dos conceitos

³ A positivação expressa do direito fundamental à proteção de dados pessoais no rol de direitos e garantias fundamentais do artigo 5º da Constituição Federal, a partir do ano de 2022, não afasta a relevância substancial do direito à proteção de dados pessoais, elemento apto a lhe conferir, antes da EC 115, fundamentalidade material, especialmente porque, na atualidade, não é difícil a demonstração da importância dos valores, princípios e direitos fundamentais associados à proteção de dados, tanto para a esfera individual, quanto para o interesse coletivo. Consubstanciando este entendimento foi a decisão proferida monocraticamente pela Ministra Rosa Weber no ano de 2020, posteriormente referendada pelo Plenário do Supremo Tribunal Federal, no julgamento da Ação Direta de Inconstitucionalidade nº 6.387/2020, reconhecendo a existência de um direito fundamental autônomo à proteção de dados pessoais.

de dados pessoais e inteligência artificial acarretam uma necessária tensão entre ambos (OLIVEIRA; DIAS, 2023, p. 151). De um lado, os sistemas de inteligência artificial sendo alimentados por imensas quantidades de dados, e de outro lado, as regras de proteção de dados condicionando o modo como a inteligência artificial pode e deve tratar os dados pessoais.

No âmbito da União Europeia, desde 2021, tramita Proposta de Regulamento da Inteligência Artificial (*AI Act*), a qual tem por um de seus objetivos o estabelecimento de regras harmonizadas em matéria de inteligência artificial, melhorando as previsões, otimizando as operações e personalizando o fornecimento de serviços. Em sentido mais específico, e considerando que a Proposta apresenta natureza horizontal, isto é, exige plena coerência com a legislação da União Europeia, garante um complemento – não um prejuízo (OLIVEIRA; DIAS, 2023, p. 152) – à matéria de proteção de dados, notadamente o *General Data Protection Regulation (GDPR)*. Trata-se de desenvolver e organizar regras harmonizadas aplicáveis a ambas as temáticas.

A Proposta da União Europeia já serve como marco jurídico inspirador para a regulamentação da temática em diversos ordenamentos jurídicos ao redor do mundo, incluindo o Brasil. Efetivamente, a ideia que permeia o *AI Act* está em tentar ultrapassar, ou ao menos minimizar, a tensão que necessariamente existe entre proteção de dados pessoais e inteligência artificial.

O ordenamento jurídico brasileiro conta, desde 2020, com a Resolução nº 332 do Conselho Nacional de Justiça, que, dentre outras providências, dispõe sobre a ética, a transparência e a governança na produção e no uso de inteligência artificial no Poder Judiciário. Em um sentido mais amplo há, também, tramitando no Congresso Nacional, o Projeto de Lei nº 21/2020, que visa a criação do Marco Legal da Inteligência Artificial, a partir do estabelecimento de fundamentos, princípios e diretrizes para o desenvolvimento e a aplicação da inteligência artificial no Brasil. É de se destacar, também, a Portaria nº 4.671/2021, do Ministério da Ciência, Tecnologia e Inovação, que instituiu a Estratégia Brasileira de Inteligência Artificial.

A Lei Geral de Proteção de Dados brasileira, por sua vez, tal qual o Regulamento Geral de Proteção de Dados da União Europeia, não trata de forma específica e expressa sobre a inteligência artificial. Em contrapartida, tais

legislações, ao regulamentarem e permitirem a possibilidade de controle dos dados pessoais por seus usuários, o que se soma, no Brasil, ao fato de que, salvo exceções expressamente previstas em lei, instituições públicas e privadas devem se submeter às disposições da LGPD, faz com que seja preciso considerar a necessidade de submissão das inteligências artificiais também a estas noções.

Hodiernamente, fato é que a problemática está muito mais na busca por boas práticas voltadas ao aperfeiçoamento ético e transparente das tecnologias inteligentes, do que propriamente no aprimoramento destas tecnologias, pois tal já ocorre em uma velocidade alarmante (PINTO; ERNESTO, 2022, p. 438). Nesse contexto, um dos principais desafios da Lei Geral de Proteção de Dados está em regular, de forma ética e transparente, a atividade de inteligência artificial sobre o tratamento de dados pessoais, especialmente enquanto não consolidada uma legislação específica sobre a temática.

O texto da Lei Geral de Proteção de Dados brasileira dispõe, de forma específica, que o titular tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses. O direito à explicação, que emana no artigo 20, decorre do princípio da transparência, disposto também expressamente na Lei. Não há como negar, porém, que há uma perceptível fragilidade e insuficiência da LGPD para lidar com o *big data* e a alta complexidade e possibilidade de processamento de dados que, por sua vez, influenciam a nova realidade de tomada de decisões apoiada em inteligência artificial.

Fato é que se antes o sistema focava muito mais na perspectiva da autodeterminação informacional, agora está muito mais em torno de processos de gerenciamento dos riscos que envolvem as atividades de tratamento de dados (BIONI, 2019, p. 215). Assim, ao se tratar da relação entre Inteligência Artificial e Direito, passa a ser preciso superar a noção costumeira que tem por foco os potenciais de vigilância (HOFFMANN-RIEM, 2019, p. 13).

Dentro desta ideia, não se está cogitando em colisão jurídica ou substituição normativa, mas sim uma nova tipologia, decorrente da necessidade de mecanismos focados na identificação e na mitigação de incertezas e possíveis prejuízos que decorrem do tratamento dos dados pessoais (ZANATTA, 2017, p. 181). Significa

reconhecer que a proteção de dados pessoais tem passado por significativas transformações, mantendo, por seu inestimável valor, a noção de autodeterminação informacional, mas agregando ao seu conjunto a ideia de mitigação de riscos.

CONCLUSÕES

Já é de conhecimento geral que o mundo tem passado por profundas transformações, em especial as de caráter tecnológico e computacional, contexto em que a inteligência artificial, baseada em algoritmos e *big data*, ocupa posição de destaque. Em contrapartida, não são incomuns as reações de espanto no que diz com a velocidade das inovações tecnológicas e com o impacto delas na vida em sociedade.

O momento merece reflexão e atenção, tendo em vista que são incontáveis os riscos associados ao viés algorítmico e à discriminação na tomada de decisões. A mitigação dos erros começa com um *design* responsável, a partir da adoção de práticas éticas e de transparência, para garantir que a inteligência artificial seja uma força positiva para a sociedade em geral.

Como visto, é importante que a transparência e o *accountability* em sistemas de IA devam ser garantidos não apenas por meio de normas e regulamentos, mas também por meio da adoção de uma cultura de ética e transparência no desenvolvimento e no uso dessas tecnologias, seja a partir de uma ética e privacidade *by design* ou pelo combate ao enviesamento discriminatório nocivo. Isso envolve a promoção de uma ampla participação dos usuários, a transparência nas práticas de coleta e uso de dados e a promoção de processos de avaliação e revisão constantes. Somente assim será possível garantir que os sistemas de IA sejam utilizados de forma responsável e que contribuam efetivamente para o bem-estar da sociedade.

Ademais, como se pode perceber, a Lei Geral de Proteção de Dados brasileira parece não ser suficiente para abarcar o cenário como posto hoje, especialmente em razão da perceptível mudança de foco, que está mais no gerenciamento de riscos que envolve as atividades de tratamento de dados, do que propriamente em uma preocupação com a vigilância e autodeterminação informacional. Daí a importância

de uma legislação específica sobre a temática, apta a conferir sistematização e capacidade formal e material de tutela, efetivando a relação entre Inteligência Artificial e Direito.

Os desafios das novas normativas sobre Inteligência Artificial deverão superar os desafios aqui postos, além daqueles que naturalmente ocorrem, e outros que foram abordados *en passant* no presente *paper*. O que fica, no entanto, é que os aspectos éticos humanos devem ser reforçados e aumentados para a sua associação ao núcleo determinante das programações das funcionalidades das aplicações de IA. As IAs devem ter um aperfeiçoamento maior a cada breve momento nos próximos anos, e isso deve ser incentivado e explorado ao máximo em prol da humanidade. Mas é em prol da humanidade, e não de interesses que objetificam o ser-humano como mero insumo na cadeia produtivo-econômica. A tarefa do jurista do atual tempo é de ter a capacidade de acompanhar e entender as potentes revoluções que ocorrem em termos de tecnologia, avaliar em quais pontos impactam em direitos, sobretudo em direitos fundamentais, em termos de Brasil, e estruturar defesas e recomendações para a garantia de uma evolução tecnológica com acompanhamento evolutivo social. Eis a ética para um novo despertar robótico dos seres humanos, em que máquinas auxiliam a vida humana, e não a dificultam. Quando acabam por dificultá-la, o remédio imediato é o mesmo: transparência, para que daí decorra explicabilidade, ética e ajustes.

REFERÊNCIAS

BIONI, Bruno Ricardo. LUCIANO, Maria. O princípio da precaução na regulação de inteligência artificial: seriam as leis de proteção de dados o seu portal de entrada? FRAZÃO, Ana; MOULHOLLAND, Caitlin (Coord.). **Inteligência artificial e Direito: ética, regulação e responsabilidade**. São Paulo: Revista dos Tribunais, 2019, p. 208-231.

BUITEN, Miriam C. Towards intelligent regulation of artificial intelligence. **European Journal of Risk Regulation**, n. 10, p. 41–59, 2019.

DONEDA, Danilo. A LGPD como elemento estruturante do modelo brasileiro de proteção de dados. In: DONEDA, Danilo; MENDES, Laura Schertel; CUEVA, Ricardo Villas Bôas (Coord.). **Lei geral de proteção de dados (Lei nº 13.709/2018): a caminho da efetividade: contribuições para a implementação da LGPD**. São Paulo: Thomson Reuters do Brasil, p. 243-255, 2020.

FERRARI, Isabela; BECKER, Daniel; WOLKART, Erik Navarro. Arbitrium ex machina: panorama, riscos e a necessidade de regulação das decisões informadas por algoritmos. **Revista dos Tribunais**, v. 995, p. 635-655, set./2018.

HARARI, Yuval Noah; HARRIS, Tristan; RASKIN, Aza. O domínio da inteligência artificial sobre a linguagem é uma ameaça à civilização. **Jornal Estadão**. São Paulo, 2023. Disponível em: <<https://www.estadao.com.br/internacional/yuval-harari-o-dominio-da-inteligencia-artificial-sobre-a-linguagem-e-uma-ameaca-a-civilizacao/>>. Acesso em 26 abr. 2023.

HOFFMANN-RIEM, Wolfgang. **Teoria geral do Direito Digital: transformação digital, desafios para o Direito**. Tradução de Italo Fuhrmann. Rio de Janeiro: Forense, 2020.

HOFFMANN-RIEM, Wolfgang. Proteção de dados e inteligência artificial: perspectivas éticas e regulatórias. Tradução de Luiz Sander. **RDU**, v. 16, n. 90, p. 11-38. Porto Alegre, 2019.

LANEY, Douglas. **3D Data Management: Controlling Data Volume, Velocity, and Variety**. META Group, 2001. Disponível em: <<http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf>>. Acesso em 27 abr. 2023.

LORDELO, João Paulo. Algoritmos e direitos fundamentais: riscos, transparência e *accountability* no uso de técnicas de automação decisória. **Revista Brasileira de Ciências Criminais**, v. 186, p. 205-236. São Paulo: RT, dez., 2021.

LORDELO, João Paulo. Vieses implícitos e técnicas de automação decisória: riscos e benefícios. **Revista da ANNEP de Direito Processual**, v. 1, n. 2, art. 44, 2020.

NEGRÃO, Antônio Carlos. Economia digital, proteção de dados e competitividade. In: DONEDA, Danilo; MENDES, Laura Schertel; CUEVA, Ricardo Villas Bôas (Coord.). **Lei geral de proteção de dados (Lei nº 13.709/2018): a caminho da efetividade: contribuições para a implementação da LGPD**. São Paulo: Thomson Reuters do Brasil, p. 29-37, 2020.

O'NEIL, Cathy. **Algoritmos de destruição em massa: como o big data aumenta a desigualdade e ameaça a democracia**. Trad. Rafael Abraham. Santo André: Editora Rua do Sabão, 2020.

OLIVEIRA, Inês; DIAS, José Luís. Inteligência Artificial e proteção de dados. **Inteligência Artificial no contexto público: Portugal e Brasil**. PEDRO, Ricardo; CALIENDO, Paulo (Coord.). Coimbra: Almedina, p. 145-170, 2023.

PARANHOS, Mário C. Oliveira. **Viés algorítmico: uma análise sobre discriminações automatizadas**. Rio de Janeiro: Lúmens Juris, 2022.

PASETTI, Marcelo. Algumas reflexões no desenvolvimento da inteligência artificial ética: sua importância na regulação no Brasil. **Inteligência Artificial no contexto público**: Portugal e Brasil. PEDRO, Ricardo; CALIENDO, Paulo (Coord.). Coimbra: Almedina, p. 173-190, 2023.

PASQUALE, Frank. **The black box society**: the secret algorithms that control money and information. Cambridge e Londres: Harvard University Press, 2015.

PEIXOTO, Fábio Hartmann; SILVA, Roberta Zumblick Martins da. **Inteligência Artificial e Direito**. Coleção Direito, Racionalidade e Inteligência Artificial, v. 1. Curitiba: Alteridade, 2019.

PINTO, Henrique Alves; ERNESTO, Leandro Miranda. Inteligência artificial aplicada ao Direito: por uma questão de ética. **Revista de Processo**, v. 327, a. 47, p. 431-449. São Paulo: RT, maio, 2022.

POLONSKI, Vyacheslav. **Mitigating algorithmic bias in predictive justice**. 4 AI design principles for AI fairness, 2018.

REIS, Paulo Victor Alfeo. **Algoritmos e o Direito**. São Paulo: Almedina, 2020.

ROSSETTI, Regina; ANGELUCI, Alan. Ética algorítmica: questões e desafios éticos do avanço tecnológico da sociedade da informação. **Galáxia**, n. 46, p. 1-18. São Paulo, 2021. Disponível em: <<https://www.scielo.br/j/gal/a/R9F45HyqFZMpQp9BGTfZnyr/?format=pdf&lang=pt>>. Acesso em 26 abr. 2023.

STEINER, Christopher. **Automate This: how algorithms came to rule our world**. New York: Penguin Group, 2012.

UNIÃO EUROPEIA. Proposta de Regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de inteligência artificial (Regulamento Inteligência Artificial) e altera determinados atos legislativos da União. Bruxelas, 2021. Disponível em: <<https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52021PC0206&from=EN#:~:text=A%20propost a%20estabelece%20regras%20harmonizadas,futuro%20de%20%C2%ABintelig%C3%A2ncia%20artificial%C2%BB.>>>. Acesso em 24 abr. 2023.

VAKKURI, Ville; ABRAHAMSSON, Pekka. The Key Concepts of Ethics of Artificial Intelligence. **IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC)**, Stuttgart, p. 1-6, 2018.

YAPO, Adrienne; WEISS, Joseph. Ethical implications of Bias in Machine Learning. **Proceedings of the 51st Hawaii International Conference on System Sciences**, p. 5365-5372, 2018. Disponível em: <<https://core.ac.uk/works/17806729>>. Acesso em 28 abr. 2023.

ZANATTA, Rafael Augusto Ferreira. Proteção de dados pessoais como regulação de risco: uma nova moldura teórica? **I Encontro da Rede de Pesquisa em Governança da Internet**. Rio de Janeiro, 2017, p. 175-193. Disponível em: <http://www.redegovernanca.net.br/public/conferences/1/anais/ZANATTA,%20Rafael_2017.pdf>. Acesso em 25 abr. 2023.

3. DA INTERRELAÇÃO ENTRE DIREITO, TECNOLOGIA E GOVERNANÇA NA PROTEÇÃO DE DADOS PESSOAIS

*THE INTERRELATION BETWEEN LAW, TECHNOLOGY, AND GOVERNANCE IN
THE PROTECTION OF PERSONAL DATA*



<https://doi.org/10.36592/9786554600552-03>

*Ariel Augusto Lira de Moura*¹

*Bernardo Leandro Carvalho Costa*²

RESUMO

A Lei Geral de Proteção de Dados (LGPD) faz parte de um contexto de convergência de processos jurídicos, políticos e econômicos para lidar com os desafios impostos pelas sociedades e economias orientadas por dados. O problema é, nesse sentido, como integrar conjuntamente o vínculo entre direito e tecnologia na governança da proteção de dados pessoais. Objetiva-se explorar a relação entre direito, tecnologia e governança na proteção de dados, particularmente no contexto da LGPD. Emprega-se a metodologia pragmático-sistêmica de Leonel Severo Rocha com as técnicas de pesquisa bibliográfica e documental. O estudo conclui que as organizações não poderiam sustentar a LGPD sem adotar estruturas e padrões de segurança da informação e governança. Assim, destaca-se a necessidade de uma compreensão teórica transdisciplinar da proteção de dados no Brasil, alinhada com os pressupostos técnicos, práticos e organizacionais da cultura de rede.

Palavras-chave: Direito. Tecnologia. Governança. Proteção de Dados Pessoais. Transdisciplinaridade.

¹ Doutorando em Direito Público pelo Programa de Pós-Graduação em Direito (PPGD) da Universidade do Vale do Rio dos Sinos (UNISINOS). Bolsista PROEX/CAPES, membro do Grupo de Pesquisa Teoria do Direito (CNPq), sob orientação do Prof. Dr. Leonel Severo Rocha. Advogado (OAB/SP). Data Protection Officer e Information Security Officer (EXIN). Link do Currículo Lattes: <http://lattes.cnpq.br/9370431630574637>. Contato do correio eletrônico (e-mail): ari.moura06@gmail.com

² Doutor em Direito Público pela Universidade do Vale do Rio dos Sinos (UNISINOS) e Université Paris 1 Panthéon-Sorbonne. Professor do Centro Universitário do Vale do Araguaia (UNIVAR). Link do Currículo Lattes: <http://lattes.cnpq.br/6564157581934332>. Contato do correio eletrônico (e-mail): bernardo@digitalattractor.com.br

ABSTRACT

The Brazilian General Data Protection Regulation (LGPD) is part of a context of convergence of legal, political, and economic processes to deal with the challenges posed by data-driven societies and economies. The problem is, in this sense, how jointly integrate the link between law and technology in the governance of personal data protection. It aims to explore the relationship between law, technology, and governance in data protection, particularly in the context of the LGPD. Leonel Severo Rocha's pragmatic-systemic methodology with the bibliographic and documentary research techniques is employed. The study concludes that organizations could not sustain the LGPD without adopting information security and governance structures and standards. Thus, it highlights the need for a transdisciplinary theoretical understanding of data protection in Brazil aligned with the technical, practical, and organizational assumptions of network culture.

Keywords: Law. Technology. Governance. Personal Data Protection. Transdisciplinarity.

INTRODUÇÃO

A Lei Geral de Proteção de Dados (2018) brasileira têm sua raiz um extenso debate multissetorial (governo, academia, sociedade civil, iniciativa privada) de uma década, junto ao Marco Civil da Internet (2014). Essa transdisciplinaridade é inerente ao próprio desenvolvimento inicial e recentes transformações da governança não só brasileira como global da internet (ROCHA; MOURA, 2020). Contudo, a pressão para sua aprovação se deu concomitante a entrada em vigor do Regulamento Geral de Proteção de Dados (GDPR - *EU General Data Protection Regulation*).

Nesse sentido, a LGPD nasce, em verdade, de um contexto global de "convergência" de processos regulatórios jurídicos, políticos e econômicos para enfrentamento das novas dinâmicas da sociedade e economia movida à dados, algo que remete sua origem ao processo transnacional de construção de regulamentações sobre o tema impulsionado pela Organização para a Cooperação e Desenvolvimento Econômico (OCDE) desde o século passado (MOURA; ROCHA, 2022b).

Em um contexto geral de modificação dos modos de governança (global e digital), e, ainda, considerando que a proteção de dados pessoais possui não só as dimensões jurídica, política e econômica como, também, técnica (e.g. segurança da informação), questiona-se como a relação entre direito e tecnologia podem ser conjuntamente consideradas na governança da proteção de dados pessoais.

Objetiva-se, em um sentido geral, construir a observação conjunta entre direito, tecnologia e governança aplicada a proteção de dados pessoais. Especificamente, pretende-se refletir sobre os pressupostos técnicos e cognitivos das práticas sociais na cultura das redes, (re)construindo os modos de organização e governança e observar a interrelação entre direito, tecnologia e governança da proteção de dados na LGPD, direcionando-se uma observação adequada para refletir sobre a efetivação deste ("novo") direito.

A fim de realizar esse empreendimento, faz-se a utilização da metodologia pragmático-sistêmica de Leonel Severo Rocha (2013a) aliada as técnicas de pesquisa bibliográfica e documental, principalmente a partir de autores centrais para os debates teóricos da Teoria dos Sistemas, como Niklas Luhmann (2006), Gunther Teubner (2012) e Thomas Vesting (2018), e por meio da análise de leis, regulamentações e normas técnicas.

Essa metodologia mostra-se como um desenvolvimento epistemológico que pretende analisar os fenômenos sociais contemporâneos em toda sua complexidade. Nesse sentido, e com fins didáticos, Rocha (2013a) reconstrói as principais matrizes de observação da teoria jurídica classificando-as de acordo com sua inserção na tradicional divisão da semiótica de Carnap: sintática, semântica e pragmática. Assim, ela se posiciona como uma observação da teoria jurídica, centrada na dimensão pragmática da linguagem. Mas a incorporação da análise sistêmica em seu instrumental teórico permite que se observe não só o direito diante de seu uso linguístico, como também a comunicação jurídica em condições de incerteza.

A transdisciplinaridade, como resultado, permite navegar dentre os diversos autores (sistêmicos ou não), a fim de que se observe, por meio de uma teoria jurídica plural, o entrecruzamento entre o direito, a tecnologia e a governança na hodierna

cultura das redes com especial atenção para (re)modelação das práticas sociais e a construção dos sentidos a elas subjacentes (ROCHA, 2005).

Por fim, a pesquisa justifica-se, primeiramente, pela própria necessidade de um entendimento teórico aprofundado e transdisciplinar no campo da proteção de dados pessoais. Considerando a ainda falta de maturidade da temática no âmbito brasileiro, não só no campo das organizações (cultura organizacional), a aplicação da análise teórica para observação da relação entre dispositivos da LGPD e as normas ISO pode trazer luz a questões práticas para sua sustentação.

1 DIREITO, ORGANIZAÇÕES, ESTADO E CULTURA DAS REDES

A Teoria dos Sistemas de Niklas Luhmann é um excelente ponto de partida para observação da sociedade global e digital, já que a própria modernidade é descrita por meio do processo de diferenciação funcional da sociedade mundial, o sistema social que abarca todas as comunicações ("omniabarcador"). Nesse sentido, Direito, Política e Economia são sistemas sociais parciais e globais de comunicação que se diferenciam entre si pela função que exercem na sociedade: o resguardo jurídico de expectativas, o asseguramento futuro diante da escassez dos bens e o decidir coletivamente vinculante, respectivamente (LUHMANN, 2006). Na teoria "pós-ontológica" de Luhmann, não se busca pelo "fundamento último" dos sistemas, ou, ao menos, ele não é algo externo ou transcendental. (CLAM, 2006).

Da (auto)evidência de uma sociedade mundial, a partir do "fato" da globalização, como afirmava Luhmann (1997), soma-se o crescimento do uso do computador e a constante migração das práticas sociais para novos espaços de sociabilidade construídos no interior da Internet. Para Luhmann (1990; 2006) estava claro que as consequências da introdução do computador na sociedade seriam o verdadeiro teste de utilidade para sua teoria. Mas ele estava preparado em grande medida para os avanços da comunicação em rede.

Isso pela própria insistência na epistemologia do construtivismo (operativo), que fora construída a partir da informática e da cibernética, amparada pela observação da sociedade (*i.e.* comunicação) como um evento improvável, cujo próximo passo sempre estava por ser gerido, e, como uma teoria da diferença,

fornece não só um ponto de partida para a teoria dos computadores, mas também para uma “teoria dos computadores-em-sociedade” (BAECKER, 2006a). A questão da validade de um direito que opera de maneira recursiva “[...] determinando vizinhanças em forma de redes”, como afirmava Luhmann (2016, p. 192), por exemplo, está conectada ao início do que denominaremos, com Vesting (2015), de cultura das redes.

Mas sua teoria diz respeito não só a diferenciação de sistemas funcionais de sentido (direito, política, economia) como também sistemas de interação (entre presentes) e organizações. As organizações, para ele, são sistemas autopoieticos que se diferenciam pela tomada de decisão. A partir desta atividade, as organizações tratam a incerteza inerente a realidade social. Após a “[...] dissolução dos marcos de referência da certeza”, como diria Lefort (1991, p. 34), a forma de sociedade moderna teve de lidar com a indeterminabilidade inerente à tomada de decisões sempre diferentes, já que “[...] não se pode mais pensar em critérios de verdade necessária ou impossível; mas somente possível”. (ROCHA, 2013b, p. 13).

Elas se localizam-se no centro dos sistemas funcionais (tribunais, burocracia estatal, bancos) e realizam a “tradução” ou “relação” entre os indivíduos (sistemas psíquicos) e os sistemas funcionais, o que traz um instrumental teórico eficaz para se pensar as questões sobre o papel das organizações na proteção de dados e os modos de sua governança. (LUHMANN, 2010; 1993). Dito de outro modo, as organizações estão entre o nível “micro” e “macrossociológico” e tem um papel fundamental na estruturação das relações entre indivíduos e sistemas, entre “titulares de dados” e os diversos setores sociais modificados pela digitalização.

Em (des)continuidade, Teubner (2002; 1996) observara novos regimes de governança no direito global para além do Estado, novos espaços de tomadas de decisões jurídicas, políticas e econômicas, principalmente após a queda do muro de Berlim (1989). Mas aquilo que se pode descrever como a proliferação de regimes de “governança global”, para além das lógicas nacionais e regionais, já envolvem os próprios âmbitos políticos, econômicos e jurídicos a muito tempo a partir de regimes de padronização (técnicos) – como é o caso, por exemplo, da Organização Internacional de Padronização (ISO – *International Organization for Standardization*).

Nesse ponto, deve-se ressaltar que se nos processos econômicos o processo contratual é a “instituição de ligação” (“conexão” e “diferenciação”), nos processos técnicos, científicos e médicos é a padronização a instituição de ligação com o direito. Os processos de padronização global (do comércio, do transporte e comunicação) conectam-se à gestão das incertezas técnicas e jurídicas nas organizações, apresentando-se como uma importante lógica para os processos globais.³ Nesse sentido, afirma Teubner (2004, p. 78):

Os processos de padronização global, que surgem em parte através das forças de mercado, em parte através do estabelecimento interno em organizações internacionais, em parte através de negociações entre atores privados e públicos, estão entre as fontes mais importantes do direito global. Se os padrões cognitivos científicos, técnicos ou médicos são normalizados e, em última instância, juridicamente vinculativos, então também aqui a lei desenvolveu uma mistura adequada de distância e adaptação em relação à ciência e à tecnologia. A despoliticização das decisões legislativas corresponde a uma “descienciização” das normas⁴ (tradução nossa).

Dando um passo além, pode-se afirmar que este “fenômeno” reestrutura até mesmo as “questões constitucionais” atuais (organização do poder e a proteção de direitos fundamentais). (ROCHA; COSTA, 2018; 2021). Na linha de Teubner (2009; 2012), por exemplo, os códigos corporativos de multinacionais são um claro exemplo de um processo de evolução autorregulatória que passa a estruturar juridicamente (“autoconstituição”/“auto-organização”) a governança corporativa das organizações em direção a sua “responsabilidade social” e a proteção de direitos fundamentais por mecanismos internos (“auto-limitação”).

³ O campo da comunicação é central neste sentido, bastando-se verificar que a primeira grande organização internacional é precisamente a União Internacional de Telecomunicações (UIT), fundada em 1865, e anexada à ONU (Organização das Nações Unidas) em 1947.

⁴ “Global standardization processes, coming about partly through market forces, partly through being laid down internally in international organizations, partly through negotiations between private and public actors, are among the most important sources of global law. If scientific, technical or medical cognitive standards are normed and ultimately juridified, then here too the law has developed an adequate mixture of distance and adaptation vis-à-vis science and technology. The depoliticization of legislative decisions corresponds to a ‘desciencification’ of standards”.

Levando-se para as transformações no interior do Estado, Teubner (1993), ao observar as transformações políticas, jurídicas e econômicas, ainda na década de 1980, já descrevia um processo de “[...] mudança de arranjos macrocorporativistas centralizados para redes mais flexíveis, descentralizadas e plurais do policorporativismo” com a posterior mudança em direção à um “Estado em Rede”, cujo papel é facilitar o desenvolvimento organizacional e a institucionalização de um status público por meio do redesenho na autorregulação de organizações intermediárias privadas (GOLIA; TEUBNER, 2021).

Vesting (2018), em um sentido complementar, a partir da teoria das mídias, constrói a tese de que a partir do surgimento e do uso do computador e as novas tecnologias alteram os pressupostos técnicos e cognitivos das práticas sociais na atual cultura das redes. A partir desta base pode-se observar as modificações das interrelações entre indivíduos, organizações, sistemas, redes e tecnologia. Principalmente se se considerar que as práticas sociais estavam assentadas em uma forma de “conhecimento comum” (compartilhado) que não pode mais ser facilmente encontrado na sociedade atual, já que, como afirma Ladeur (2016, p. 160), o “[...] campo das novas tecnologias complexas [...] se baseia em um tipo de conhecimento que se distanciou do conhecimento geral acessível à experiência”.

O atual “Estado em Rede”, nesse sentido, teria como papel reunir experiências de várias ordens fragmentadas na tentativa de (co)gerar novos padrões de (auto)organização das práticas sociais, já que não é mais possível centralizar essa tarefa em apenas um “ponto” (indivíduo, organização, sistema) (VESTING, 2022). Por essa razão, argumenta-se que a regulação da proteção de dados pessoais deve seguir uma forma de direito “proceduralizado”, a partir do modelo da autorregulação regulada, no qual “[...] procedimentos sejam criados para compreender a incerteza e gerar conhecimento sobre a persecução de certos objetivos e interesses públicos estabelecidos” (ABBOUD; CAMPOS, 2018, p. 35).

2 DIREITO, TECNOLOGIA E GOVERNANÇA NA PROTEÇÃO DE DADOS PESSOAIS

Explica-se que as teorias de governança (corporativa), originadas no âmbito econômico em 1970, passam a invadir o campo de reflexão da ciência política e,

nesse sentido, a governança estatal passou a ser cada vez mais caracterizada de modo mais “negocial” e “heterárquico” em diversas áreas do conhecimento. A teoria do direito, preocupada, tradicionalmente, com a validade (interna) de expectativas normativas, amplia sua atenção para com os efeitos sociais da regulação jurídica, abrindo um maior diálogo para com as ciências sociais (e econômicas) (BORA, 2017).

“Governança”, nesse sentido, é o conceito que engloba novas formas de conexão institucional em rede de diversos atores em uma multiplicidade de contextos sociais, sendo a “regulação” uma parte específica da governança “[...] que lida com a direção de eventos e estados de coisas”⁵ (BORA, 2015, p. 144, tradução nossa). A partir do exposto, o que não se pode perder de vista é que a criação de zonas cinzentas entre o público e o privado não está necessariamente relacionado a um “encolhimento do Estado”, mas sua reorganização e conexão em rede com outras organizações para governança e regulação de novos temas e problemas, como a proteção de dados pessoais.

A governança e regulação da proteção de dados pessoais, nesse sentido, segue um modelo de redes, de modo que o Estado, por meios de organizações próprias (e.g. Autoridade Nacional de Proteção de Dados e ANS), regulamenta os pressupostos da (autor)regulação de organizações (e.g. hospitais, clínicas) e os modos de governança de setores específicos (e.g. saúde). Ademais, como disserta Graber (2021) há uma necessária complementariedade entre as observações jurídicas (e dos juristas) com as observações das ciências da tecnologia (e os cientistas) para o necessário aprendizado recíproco das problemáticas envolvidas à sociedade em rede – e.g. proteção de direitos fundamentais no âmbito digital e/ou diante das novas tecnologias (MOURA; ROCHA, 2022a).

Não por acaso a governança da proteção de dados pessoais se conecta, em um contexto técnico-organizacional mais amplo, à inúmeros padrões e *frameworks* globais de, por exemplo, gestão de risco (e.g. ISO/IEC 27005:2018 e ISO/IEC 31000:2018), de segurança da informação (e.g. a família ISO/IEC 27000 e o *NIST Cyber Security Framework*), da governança da Tecnologia e da Informação (e.g.

⁵ “[...] which deals with the steering of events and states of affairs”.

COBIT 2019) e/ou de governança de dados (e.g. DAMA-DMBOK) (KYRIAZOGLU, 2016) (ITGP, 2020).

A ISO/IEC 27701:2019, de gestão da privacidade, por exemplo, é reconhecida não só no âmbito europeu, por exemplo, como também no Brasil a partir do ressonante entendimento consolidado pelo TCU no TC 039.606/2020-1 – com o diagnóstico do grau de implementação da lei geral de proteção de dados na administração pública federal. (BRASIL, 2022). Esta norma técnica é uma extensão da norma antes citada para desenvolvimento de um sistema de gerenciamento de segurança da informação. Assim, a padronização técnica (e tecnológica) e os *frameworks* de boas práticas produzem materiais de sentido que não podem ser dispensados pelo direito e o Estado.⁶

Para proteção e efetivação do direito fundamental à proteção de dados pessoais, e todos os direitos a eles conexos, principalmente a partir do “paradigma” da “autodeterminação informativa”, necessita-se de medidas técnicas (e.g. autenticação segura, criptografia, proteção contra malware, segurança de redes) e organizacionais (e.g. gestão de *logs*, direitos de acesso, gestão do conhecimento, políticas internas, canais de denúncia, conscientização e treinamentos) adequadas, como prescreve a própria LGPD em seu artigo 46⁷ e que se reverbera por todo o texto normativo consolidando-se por meio das boas práticas e da governança (Capítulo VII, Seção II)⁸ (MENDES, 2020) (BRASIL, 2020).

Assim, a exemplo, não se pode pensar a dimensão jurídico-regulatória, a obrigatoriedade de se estrutura planos de resposta e remediação de incidentes sem se pensar em *frameworks* de boas práticas como o ITIL (*Information Technology*

⁶ Vide o artigo 51 da LGPD (BRASIL, 2020): “A autoridade nacional estimulará a adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais”.

⁷ “Os agentes de tratamento devem adotar medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito”.

⁸ “Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais”.

Infrastructure Library) e a ISO/IEC 20000 de gerenciamento de serviços de TI⁹ ou, em um sentido mais amplo, a própria integração responsável e consciente do “negócio” com a “tecnologia” a partir do COBIT 2019 (*Control Objectives for Information and Related Technologies*)¹⁰ e a utilização de sistemas internos para monitoramento constante.

A criptografia, como um “direito”, que junta a toda complexidade que implica sua regulação – desde questões de segurança pública até mesmo a sua (in)efetividade diante da computação quântica – é um excelente exemplo nesse sentido (WIMMER; MORAES, 2022). (SAAVEDRA; SALES; PEREIRA, 2020). Assim como a construção jurídico-dogmática alemã do direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais que complementa, reforça, estrutura a proteção da autodeterminação informativa e o livre desenvolvimento da “pessoa” em um contexto de digitalização da realidade social (MENKE, 2019).

A relação entre Direito e tecnologia, reestrutura-se a partir de novos modos de se governar o próprio social. A proteção de dados pessoais, nesse sentido, se conecta a uma rede de atores envolvidos na remodelação da governança e regulação de processos tecnológicos de diversas ordens. Basta-se pensar, no campo da saúde, em homenagem a este evento, que a preocupação com a proteção de dados sensíveis diante da revolução tecnológico-digital para os serviços (e.g. telemedicina e a impressão 3D de próteses) e pesquisas na área da saúde (e.g. aprendizado de máquina para descobrir novos padrões em doenças ou identificar sua evolução em

⁹ As práticas e normas técnicas envolvem o desenvolvimento de processos para o gerenciamento de incidentes (identificação, registro, classificação, priorização de incidentes e a comunicação para os titulares), gerenciamento de problemas (análise dos incidentes de segurança para identificar as causas raiz e a implementação de medidas preventivas para evitar incidentes futuros), gerenciamento de mudanças (avaliação do impacto das mudanças na segurança da informação e a implementação de medidas de segurança adequadas), gerenciamento de acessos (implementação de políticas de senha, a definição de permissões de acesso e o monitoramento do acesso aos sistemas de informação) e gestão da continuidade do serviço para garantir a disponibilidade dos sistemas de informação em caso de interrupções.

¹⁰ O COBIT 2019 pode ajudar na governança da proteção de dados pessoais fornecendo uma estrutura para identificação de riscos, o estabelecimento de controles, a garantia das conformidades regulatórias e internas, a estabelecimento de um quadro de responsabilidade e o monitoramento do desempenho do sistema, sendo um framework altamente flexível e adaptável às necessidades específicas de cada setor e organização a partir do seu “esquema” de escalonamento de objetivos gerais e específicos.

indivíduos específicos) conecta-se a necessidade não só de se estabelecer marcos regulatórios que garantam a segurança no uso dessas tecnologias como também à atenção aos impactos “ecológicos” (ambientes naturais, psíquicos e sociais) e como pode-se garantir a não dependência total das próprias tecnologias (ROCHA, 2014).

Na hodierna “cultura das redes”, contexto no qual a “esfera pública digital” e a própria “individualidade dos indivíduos” passaram a serem constantemente redimensionadas pela comunicação digital e os processos artificiais dessa realidade, a autodeterminação (“soberana”) é extremamente problemática, assim como a própria diferenciação antes fundamental entre público e privado (VESTING, 2016). Diante desses pressupostos, a “autodeterminação informacional” deve ser entendida como um direito procedimental de “controle” das pessoas sobre o fluxo de seus dados no meio em que eles circundam, já que eles (os dados) figuram, hoje, como o elemento primordial de “tradução” (construção) da subjetividade (“personalidade”) nos meios digitais (VESTING, 2018) (NISSENBAUM, 2010).

O “re-desenho” das organizações deve ser orientado, dessa forma, pela relação entre a ampliação de tecnologias de governança e gestão e a adoção de formas mais “sutis” de comunicação organizada, pois o ganho comunicacional e tecnológico só tem seu sucesso se consegue incluir a percepção (sistemas psíquicos) (BAECKER, 2006b). Isso fica claro quando se pensa na relação entre o *privacy (and security) by design*¹¹ e o correspondente aumento de capacidade de inclusão (“participação” e “controle”) dos indivíduos (“titulares de dados”) na (auto)regulação (regulada) e (auto)governança (“responsável”) dos processos comunicacionais nos novos meios sociais (e.g. plataformas) (CAVOUKIAN, 2006).

As situações de novos desenvolvimentos tecnológicos e a obrigatoriedade dos relatórios de impacto a proteção de dados pessoais, com a estruturação da gestão dos riscos, por exemplo, ou os próprios casos de divulgação de incidentes de segurança ou das próprias sanções e “achados” de fiscalizações mostram que uma “cultura da proteção de dados” só pode ser desenvolvida com a transparência e

¹¹ Vide artigo 46, § 2º, LGPD: “As medidas de que trata o caput deste artigo [medidas de segurança, técnicas e administrativas] deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

responsividade correlata ao aumento da capacidade tecnológica e sua aplicação para a própria gestão.

CONCLUSÕES

A Lei Geral de Proteção de Dados brasileira (2018) não pode ser sustentada pelas organizações sem *frameworks* e *estândares* como os acima referidos, basta uma leitura cuidadosa do próprio texto para se verificar o conjunto de prescrições que se referem a medidas técnicas e organizacionais que demandam os sentidos sedimentados (e também mutáveis) entre as práticas sociais e tecnológicas.

As inúmeras medidas de prestação de contas para a Autoridade Nacional (ANPD) e para os titulares de dados, desde relatórios de impacto a proteção de dados à incidentes de segurança que impactam os direitos e liberdades fundamentais, assim como as prescrições acerca das medidas técnicas (de segurança da informação e cibersegurança), mostram como a dimensão jurídico-normativa (Direito) conecta-se com a dimensão tecnológica por meio de uma construção granular (e transparente) de governança.

Prestação de contas, responsabilidade social e toda a sustentação da proteção de dados pessoais, nesse sentido, não se sustentam sem um contexto organizacional adequado de gestão e governança, o qual, inclusive, diz respeito não só internamente às organizações (públicas e privadas) como também às suas conexões para governança em rede e regulação de setores específicos do social. Por isso a relação entre direito e tecnologia modifica-se e conecta-se a partir dos novos modos de governança do próprio social (digital).

Assim, a interrelação entre direito, tecnologia e governança na proteção de dados pessoais pode ser observada a partir dos pressupostos técnicos e cognitivos que (re)estruturam as práticas sociais, a construção dos sentidos e a (re)organização dos modos de governança da sociedade atual em uma necessária complementariedade entre as observações e conhecimentos jurídicos e técnicos.

Dado o deslocamento do conhecimento da experiência comum acessível e compartilhada entre os indivíduos, os *frameworks* e os padrões não só auxiliam na geração de material cognitivo para regulação jurídica e a autorregulação (regulada)

nas organizações públicas e privadas, como também para “conscientização” (e com o tempo, para consolidação de uma “cultura”) dos titulares de dados sobre as dinâmicas da sociedade atual (movida a dados).

REFERÊNCIAS

ABBOUD, Georges; CAMPOS, Ricardo. A autorregulação regulada como modelo do Direito proceduralizado: regulação de redes sociais e proceduralização. *In*: ABBOUD, Georges; NERY JUNIOR, Nelson; CAMPOS, Ricardo (coord.). **Fake news e regulação**. São Paulo: Thomson Reuters Brasil, 2018. p. 19-39.

ALBERS, Marion; SARLET, Ingo Wolfgang (ed.). **Personality and Data Protection Rights on the Internet: Brazilian and German approaches**. [S.l.]: Springer, 2022.

BAECKER, Dirk. Niklas Luhmann in the society of the computer. **Cybernetics & human knowing: a journal of second-order cybernetics, autopoiesis, and cyber-semiotics**, Exeter, v. 13, n. 2, abr./jun. 2006a, p. 25-40. Disponível em: bit.ly/3UITq16. Acesso em: 10 nov. 2022.

BAECKER, Dirk. The design of organization in society. *In*: SEIDL, David; BECKER, Kai Helge. **Niklas Luhmann and organization studies**. Frederiksberg: Copenhagen Business School Press, 2006b. p. 191-204.

BORA, Alfons. The Shadow of the Law: Intermediary institutions and the ruling part of governance. *In*: HARTMANN, Eva; KJAER, Poul. **The evolution of intermediary institutions in Europe: from corporatism to governance**. Houndmills; Basingstoke; Hampshire; New York: Palgrave MacMillan, 2015. p. 141-157.

BORA, Alfons. Semantics of ruling: reflective theories in regulation, governance and law. *In*: PAUL, Regine (et al.). **Society, regulation and governance: new modes of shaping social change**. Cheltenham; Northampton: Edward Elgar, 2017. p. 15-38.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: <https://bit.ly/3Wq8Kkn>. Acesso em: 1 mar. 2023.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: <https://bit.ly/3WjVWfz>. Acesso em: 1 mar. 2023.

BRASIL. Supremo Tribunal Federal. **Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade 6.390**. Medida Cautelar em Ação Direta De Inconstitucionalidade. Referendo. Medida Provisória nº 954/2020. Emergência de saúde pública de importância internacional decorrente do novo coronavírus (Covid-

19). Compartilhamento de dados dos usuários do serviço telefônico fixo comutado e do serviço móvel pessoal, pelas empresas prestadoras, com o Instituto Brasileiro de Geografia e Estatística (IBGE). Fumus boni juris. Periculum in mora. Deferimento. Requerente: Partido Socialismo e Liberdade (P-SOL). Intimado: Presidente da República. Relatora: Ministra Rosa Weber, 7 de maio de 2020. Disponível em: <https://bit.ly/3WpYwAv>. Acesso em: 1 mar. 2023.

BRASIL. Tribunal de Contas da União. **TC 039.606/2020-1**. Grupo I – Classe V – Plenário. Relator: Augusto Nardes. Data da Sessão: 15/6/2022 – Ordinária. Disponível em: <https://bit.ly/3DTUNDY>. Acesso em 1 mar. 2023.

CAVOUKIAN, Ann. The 7 Foundational Principles Implementation and Mapping of Fair Information Practices. **Information & Privacy Commissioner**. Nov. 2006. Disponível em: <https://bit.ly/3Ws2icD>. Acesso em: 1 mar. 2023.

CLAM, Jean. **Questões fundamentais de uma teoria da sociedade**: contingência, paradoxo, só-efetuação. São Leopoldo: UNISINOS, 2006.

GRABER, Christoph B. How the law learns in the digital society. **Law, Technology and humans**, v. 3, n. 2, 2021. Disponível em: <https://lthj.qut.edu.au/article/view/1600>. Acesso em: 10 out. 2022.

GOLIA, Angelo; TEUBNER, Gunther. Networked statehood: an institutionalised self-contradiction in the process of globalisation? **Max Planck Institute for Comparative Public Law & International Law (MPIL)**, research Paper n. 2020-40, March 16, 2021. p. 7-43. Disponível em: <https://www.tandfonline.com/doi/full/10.1080/20414005.2021.1927608>. Acesso em: 1 fev. 2023.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **Tecnologia de informação - Técnicas de segurança - Gestão de riscos de segurança da informação**. ISO/IEC 27005:2018. 2018.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **Tecnologia da informação - Gestão de serviços - Parte 1: Requisitos do sistema de gestão de serviços**. ISO/IEC 27000-1:2018. 2018.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO 31000:2018. Gestão de riscos - Diretrizes**. ISO/IEC 31000:2018. 2018.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **Tecnologia da informação - Técnicas de segurança - Extensão do sistema de gestão da privacidade da informação para os requisitos da ISO/IEC 27001 e a privacidade da informação - Requisitos**. ISO/IEC 27701:2019. 2019.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **Information security, cybersecurity and privacy protection - Information security management systems -**

Requirements. ISO/IEC 27001:2022. 2022.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **Information security, cybersecurity and privacy protection - Information security controls.** ISO/IEC 27002:2022. 2022.

IT GOVERNANCE PRIVACY TEAM (ITGP). **EU General Data Protection Regulation (GDPR):** an implementation and compliance guide. 4. ed. Cambridgeshire: IT Governance Publishing, 2020.

KYRIAZOGLU, John. **Data protection and privacy management system:** data protection and privacy guide. v. 1. [S.l]: bookboon, 2016.

LADEUR, Karl-Heinz. Crítica da Ponderação na Dogmática dos Direitos Fundamentais: apelo para uma renovação da teoria liberal dos direitos fundamentais. *In:* CAMPOS, Ricardo (org.). **Crítica da ponderação:** método constitucional entre dogmática jurídica e a teoria social. São Paulo: Saraiva, 2016. p. 130-225.

LEFORT, Claude. **Pensando o político:** ensaios sobre democracia, revolução e liberdade. Rio de Janeiro: Paz e Terra, 1991.

LUHMANN, Niklas. Interaction, organization, and Society. *In:* LUHMANN, Niklas. **The differentiation of society.** New York: Columbia University Press, 1982. p. 69-89.

LUHMANN, Niklas. The cognitive program of constructivism and a reality that remains unknown. *In:* KROHN, Wolfgang; KÜPPERS Günter; NOWOTNY, Helga (ed.). **Selforganization:** portrait of scientific revolution. [S.l]: Springer, 1990, p. 64-85. Disponível em: <https://bit.ly/2HINrOJ>. Acesso em: 1 mar. 2023.

LUHMANN, Niklas. **Risk:** a sociological theory. Berlin; New York: De Gruyter, 1993.

LUHMANN, Niklas. Globalization or World society: how to conceive of modern society? **International Review of Sociology**, v. 7, n. 1, 1997. p. 67-79. Disponível em: bit.ly/3ObAWUI. Acesso em: 1 mar. 2023.

LUHMANN, Niklas. **La sociedad de la sociedad.** Ciudad de México: Herder, 2006.

LUHMANN, Niklas. **Organización y decisión.** Ciudad del México: Universidad Iberoamericana; Herder, 2010.

LUHMANN, Niklas. **O direito da sociedade.** São Paulo: Martins Fontes, 2016.

MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a história de um conceito. **Pensar - Revista de Ciências Jurídicas**, Brasília, v. 25, n. 4, set./dez. 2020. p. 1-18. Disponível em: <https://bit.ly/3zwBtKp>. Acesso em: 1 mar. 2023.

MENKE, Fabiano. A proteção de dados e o direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. **Revista Jurídica Luso-Brasileira**, Lisboa, n. 1, 2019. p. 781-809. Disponível em: <https://bit.ly/3SW7X7J>. Acesso em: 1 mar. 2023.

MOURA, Ariel Augusto Lira de; ROCHA, Leonel Severo. Direitos Fundamentais e redes sociais: Da moderação de conteúdo no Facebook ao Direito na cultura das redes. **Revista de Direito Mackenzie**, São Paulo, v. 16, n. 2, out. 2022a. Disponível em: <https://bit.ly/3Nu5hgv>. Acesso em: 1 mar. 2023.

MOURA, Ariel Augusto Lira de; ROCHA, Leonel Severo. Governança e regulação do fluxo de dados pessoais: observando os casos Schrems (TJUE). **Revista de Direito, Governança e Novas Tecnologias**, v. 8, n. 1, jan/jul. 2022b. p. 21 – 46. Disponível em: <https://bit.ly/3Dwx5wa>. Acesso em: 1 mar. 2023.

NISSENBAUM, Helen. **Privacy in context: technology, policy and the integrity of social life**. Stanford: Stanford University Press, 2010.

ROCHA, Leonel Severo. **Epistemologia jurídica e democracia**. 2. ed. São Leopoldo: Unisinos, 2005.

ROCHA, Leonel Severo. Epistemologia do direito: revisitando as três matrizes jurídicas. **Revista de Estudos Constitucionais, Hermenêutica e Teoria do Direito (RECHTD)**, v. 5, n. 2, jul./dez. 2013a, p. 141-149. Disponível em: <https://bit.ly/3kAehR6>. Acesso em: 1 mar. 2023.

ROCHA, Leonel Severo. Da epistemologia jurídica normativista ao construtivismo sistêmico II. *In*: ROCHA, Leonel Severo; SCHWARTZ, Germano; CLAM, Jean. Introdução à teoria do sistema autopoiético do direito. 2. ed. Porto Alegre: Livraria do Advogado, 2013b. p. 11-44.

ROCHA, Leonel Severo. Comunicação ecológica por Niklas Luhmann. **Revista Novos Estudos Jurídicos**, v. 19, n. 1, jan./abr. 2014. p. 232-262. Disponível em: <https://bit.ly/3f4sFQt>. Acesso em: 1 mar. 2023.

ROCHA, Leonel Severo; COSTA, Bernardo Leandro Carvalho. **Constitucionalismo social: constituição na globalização**. Curitiba: Appris, 2018.

ROCHA, Leonel Severo; MOURA, Ariel Augusto Lira de. Epistemologia das redes e a governança digital da ICANN: teoria e práxis do direito na cultura das redes. *In*: ROCHA, Leonel Severo; COSTA, Bernardo Leandro Carvalho. **Atualidade da constituição: o constitucionalismo em Luhmann, Febbrajo, Teubner e Vesting**. Porto Alegre: Fi, 2020. p. 504-538. Disponível em: <https://bit.ly/35juPXZ>. Acesso em: 1 mar. 2023.

ROCHA, Leonel Severo; COSTA, Bernardo Leandro Carvalho (org.). **O futuro da Constituição**: Constitucionalismo social em Luhmann e Teubner. Porto Alegre: Editora Fi, 2021. Disponível em: <https://bit.ly/3SWKtzt>. Acesso em: 1 mar. 2023.

SAAVEDRA, Giovani Agostini; SALES, Stela Chaves Rocha; PEREIRA, Roberta Battisti. A criptografia e seus reflexos jurídicos: estudo de caso sobre a ADPF 403 e ADI 5527 no Supremo Tribunal Federal. **Revista da Ajuris** - Associação dos Juizes do Rio Grande Do Sul, v. 47, n. 148, jan./jul. 2020. p. 129-150. Disponível em: <https://bit.ly/3DVM709>. Acesso em: 1 mar. 2023.

TEUBNER, Gunther. The "State" of private networks: the emerging legal regime of polycorporatism in Germany. **BYU Law Review**, [S.l.], v. 1993, n. 2, Apr./May 1993. p. 553-575. Disponível em: <https://bit.ly/3lBgME6>. Acesso em: 1 mar. 2023.

TEUBNER, Gunther. **Global law without a State**. Hanover: Dartmouth Publishing Company, 1996.

TEUBNER, Gunther. Breaking frames: economic globalization and the emergence of lex mercatória. **European journal of social theory**, New York, v. 5, n. 2, abr./jun. 2002, p. 199-217. Disponível em: <https://bit.ly/3lAROVE>. Acesso em: 1 mar. 2023.

TEUBNER, Gunther. Global private regimes: Neo-spontaneous law and dual constitution of autonomous sectors in world society? *In*: LADEUR, Karl-Heinz Ladeur (ed.). **Globalization and Public Governance**. Cambridge: Cambridge University Press, 2004. p. 71-87. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=894423. Acesso em: 1 mar. 2023.

TEUBNER, Gunther. The corporate codes of multinationals: company constitutions beyond corporate governance and co-determination. *In*: NICKEL, Rainer (ed.). **Conflict of Laws and Laws of Conflict in Europe and Beyond: Patterns of Supranational and Transnational Juridification**. Oxford: Hart Publishing, 2009. Disponível em: https://www.jura.uni-frankfurt.de/42852611/Generic_42852611.pdf. Acesso em: 1 mar. 2023.

TEUBNER, Gunther. **Constitutional fragments**: societal constitutionalism and globalization. Oxford: Oxford University Press, 2012.

TEUBNER, Gunther; CAMPOS, Ricardo; VICTOR, Sérgio Antônio Ferreira (org.). **Jurisprudência sociológica**: perspectivas teóricas e aplicações dogmáticas. São Paulo: Saraiva, 2020.

UNITED KINGDOM. Office of Government Commerce (OGC). **ITIL 4**. Londres: TSO - The Stationery Office, 2019.

VESTING, Thomas. Constitutionalism or legal theory: comments on Gunther Teubner. *In*: JOERGES, Christian; SAND, Inger-Johanne; TEUBNER, Gunther.

Transnational governance and constitutionalism. Oxford: Hart Publishing, 2004. p. 29-41.

VESTING, Thomas. **Teoria do direito:** uma introdução. São Paulo: Saraiva, 2015.

VESTING, Thomas. Vizinhança: direitos fundamentais e sua teoria na cultura das redes. *In:* CAMPOS, Ricardo (org.). **Crítica da ponderação:** método constitucional entre dogmática jurídica e a teoria social. São Paulo: Saraiva, 2016. p. 226-272.

VESTING, Thomas. **Legal theory and the media of law.** Cheltenham: Edward Elgar, 2018.

VESTING, Thomas. **State theory and the law:** an introduction. Massachusetts: Elgar, 2022.

WIMMER, Miriam; MORAES, Thiago Guimarães. Quantum computing, digital constitutionalism, and the right to encryption: perspectives from Brazil. **Digital Society**, v. 1, n. 2, Sep. 2022. Disponível em: <https://bit.ly/3U8Kqlc>. Acesso em: 1 mar. 2023.

4. A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD) NA PERSPECTIVA DE UMA CONSTITUIÇÃO EM REDE

THE BRAZILIAN GENERAL DATA PROTECTION REGULATION (LGPD) IN THE PERSPECTIVE OF A NETWORKED CONSTITUTION



<https://doi.org/10.36592/9786554600552-04>

Bernardo Leandro Carvalho Costa¹

Ariel Augusto Lira de Moura²

RESUMO

O presente trabalho tem como objetivos apresentar o contexto de surgimento da Lei Geral de Proteção de Dados (LGPD), destacando sua inclusão em um processo transnacional de regulamentações sobre o tema, impulsionado pela Organização para a Cooperação e Desenvolvimento (OCDE). Para tal, utiliza-se da metodologia sistêmica e da técnica de pesquisa de documentação indireta, com revisão de bibliografia nacional e estrangeira. Em aportes finais, demonstra-se o modo como as leis criadas para eventos típicos da internet, a exemplo da Lei Geral de Proteção de Dados (LGPD), estão incluídas em uma perspectiva de eficácia horizontal dos direitos fundamentais. No presente artigo, essa prática será denominada de "Constituição em Rede."

Palavras-chave: Lei Geral de Proteção de Dados (LGPD); Direitos Fundamentais; Direito Digital; Constituição;

ABSTRACT

This article aims to present the context of the emergence of the Brazilian General Data Protection Law (LGPD), highlighting its inclusion in a transnational process of regulations on the subject, driven by the Organization for Cooperation and

¹ Doutor em Direito Público (UNISINOS e Paris- 1 Panthéon Sorbonne). Membro do Grupo de Pesquisa Teoria do Direito (CNPq). Professor do Centro Universitário do Vale do Araguaia (UNIVAR). Lattes: <http://lattes.cnpq.br/6564157581934332> e-mail: bernardo@digitalattractor.com.br

² Doutorando em Direito Público pelo Programa de Pós-Graduação em Direito (PPGD) da Universidade do Vale do Rio dos Sinos (UNISINOS). Bolsista PROEX/CAPES, membro do Grupo de Pesquisa Teoria do Direito (CNPq), sob orientação do Prof. Dr. Leonel Severo Rocha. Advogado (OAB/SP). Data Protection Officer e Information Security Officer (EXIN). Link do Currículo Lattes: <http://lattes.cnpq.br/9370431630574637>. (e-mail): ari.moura06@gmail.com

Development (OECD). For this, it uses the systemic methodology and the research technique of indirect documentation, with a review of national and foreign bibliography. In conclusion, it is demonstrated how the laws created for typical internet events, such as the General Data Protection Law (LGPD), are included in a perspective of horizontal effectiveness of fundamental rights. In this article, this practice will be called "Network Constitution."

Keywords: Brazilian General Data Protection Regulation (LGPD); Human Rights; Digital Law; Network Constitution;

INTRODUÇÃO

O advento da Lei Geral de Proteção de Dados (LGPD) no Brasil é decorrente de um processo transnacional de construção de regulamentações sobre o tema. Impulsionado pela Organização para a Cooperação e Desenvolvimento (OCDE), o principal resultado desse processo foi a criação do Regulamento Europeu sobre Proteção de Dados (UNIÃO EUROPEIA, 2016).

No âmbito do Mercosul, a criação de mecanismos de regulação do tema passou a ser uma condicionante para a integração dos países membros no âmbito da Organização para a Cooperação e Desenvolvimento (OCDE).

Como consequência desse movimento, foi criada a Lei Geral de Proteção de Dados (LGPD) no Brasil (BRASIL, 2018), buscando uma aproximação com o âmbito europeu em matéria de proteção de dados pessoais.

Além da relevância da matéria tratada na legislação brasileira, há de se destacar que se trata de uma lei voltada à previsão de fatos típicos ou impulsionados pela sociedade caracterizada primordialmente pela comunicação em rede, mediada pela consolidação da internet como meio de diferenciação interna das organizações (MASCAREÑO, 2022, p. 178).

Em razão disso, à leitura e aplicação da Lei Geral de Proteção de Dados (LGPD) devem ser adicionados elementos teóricos aptos à compreensão do atual estágio de complexidade social.

Nesse sentido, o problema elencado no presente trabalho está vinculado à insuficiência das teorias tradicionais do Direito Constitucional para a leitura e

efetivação nos processos de aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD).

Em razão disso, como hipótese e resposta ao problema elencado anteriormente, buscar-se-á apresentar a concepção de Estado em Rede (VESTING, 2022, p. 185) como uma teoria apta a compreender a relação do Estado com os processos de adequação jurídica das organizações em matéria de proteção de dados pessoais.

Como aporte teórico complementar, apresentar-se-á o modo como a Constituição passa a ser aplicada de maneira não hierárquica (TEUBNER, 2018), diferenciando-se do tradicional modelo piramidal de observação (FEBBRAJO, 2016), formando uma concepção de Constituição em Rede, nos processos de adequação jurídica privilegiados pela Lei Geral de Proteção de Dados (LGPD).

O presente trabalho tem como objetivos apresentar o contexto de surgimento da Lei Geral de Proteção de Dados (LGPD), destacando sua inclusão em um processo transnacional de regulamentações sobre o tema, impulsionado pela Organização para a Cooperação e Desenvolvimento (OCDE) (COUNCIL OF EUROPE, 1981).

Ademais, com o intuito de comprovar o problema levantado no tópico anterior, objetiva-se evidenciar a diferença do tipo de regulamentação existente na Lei Geral de Proteção de Dados (LGPD) em relação às legislações tradicionais, na medida em que se trata de uma lei direcionada a fatos típicos da sociedade mediada pela comunicação em rede.

Com base nesses objetivos, o intuito do trabalho é apresentar uma concepção jurídico-constitucional adequada a compreender e efetivar os processos de adequação jurídica privilegiados pela Lei Geral de Proteção de Dados (LGPD).

A metodologia a ser aplicada é a pragmático-sistêmica (ROCHA, 2005), sobretudo a partir da Teoria dos Sistemas Sociais de Luhmann (2016).

Somam-se a essa leitura as teorias de base que aplicam a sociologia sistêmica ao Direito Constitucional, especialmente Teubner (2018) e Febbrajo (2016), bem como autores que aplicam a Teoria dos Sistemas Sociais à sociedade em rede (VESTING, 2022).

A justificativa é a utilização da matriz pragmático-sistêmica como um método apto à compreensão e criação de alternativas aos atuais problemas constitucionais (ROCHA; COSTA, 2021).

Como método de procedimento, será utilizada a técnica de pesquisa de documentação indireta, com revisão de bibliografia nacional e estrangeira.

1 A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD) NA PERSPECTIVA DE um estado em rede

O ambiente social de fragmentação constitucional que tem a internet como um novo meio de diferenciação interna dos sistemas sociais também dá guarida a formação de problemas típicos desse contexto.

Nesse sentido, de um lado, há as tradicionais organizações, que têm o condão de tomar decisões coletivamente vinculantes no âmbito dos sistemas sociais. Essas organizações atualmente são amparadas pela internet como um meio de facilitação de suas operações, apresentando-se como um mecanismo de descentralização das decisões no âmbito organizacional, na medida em que não apenas o contato com os sujeitos que acessam o sistema social resta facilitado pela internet, mas também o acesso da organização em relação a parâmetros de decisão de outras organizações.

Como destacado ao longo da pesquisa, a internet possibilita que organizações do Sistema do Direito tenham o acesso contínuo às diretrizes de âmbitos parciais especializados no tema envolvido na decisão. Esse fenômeno não apenas facilita os processos de governança e hibridismo, como também representa uma fonte de descentralização das decisões tomadas pelo tribunal.

De outro lado, surgem organizações que não são mais as tradicionais organizações do sistema social. Nesse sentido, faz-se preciso destacar o surgimento do que Vesting (2022, p. 196) tem denominado de organizações espontâneas. Trata-se de organizações encarregadas da prestação de serviços típicos da internet.

Nessa divisão, faz-se necessário destacar que algumas organizações envolvidas nessa definição já prestavam outros serviços anteriormente, mas direcionaram sua atuação para atividades tipicamente virtuais.

Em tal concepção enquadram-se as organizações especializadas em plataformas digitais. Referidas atividades não apenas facilitam as operações das organizações tradicionais, como também são indispensáveis para própria manutenção de suas prestações sociais no nível de complexidade da sociedade atual.

Como destaca Mascareño (2022, p. 100), as plataformas digitais representam um *Netdom Digital*, possibilitando o depósito de expectativas jamais antes imaginadas em relação aos diferentes sistemas sociais, cujo acesso a nível global restou facilitado pela internet.

Esse vínculo de dependência das organizações tradicionais em relação às prestações ofertadas pelas organizações espontâneas escancara o modo como o setor público, em sua tradicional acepção, resta envolvido em um vínculo de dependência com atividades prestadas por organizações do setor privado.

Não é mais possível vislumbrar a continuidade da atuação do Sistema da Política sem a intermediação de serviços de atores das organizações espontâneas. Assim, é inimaginável que o Estado não utilize os diferentes mecanismos ofertados pelas plataformas digitais.

Do mesmo modo, não se pode conceber o Sistema do Direito sem a virtualização parcial de suas atividades, sobretudo os atos dos tribunais.

Em síntese, ainda que seja válida a tradicional divisão entre público e privado, vive-se em um ambiente social em que as atividades públicas são dependentes de prestações sociais oriundas de organizações espontâneas do setor privado.

Por essa razão, é pertinente a observação de Vesting (2022, p. 217), segundo a qual os serviços prestados por essas organizações são enquadrados como atividades de interesse geral.

Todavia, ao mesmo tempo em que o Estado depende dessas atividades, faz-se importante que o Sistema da Política não perca o seu poder regulamentar no ambiente social, afinal, trata-se do sistema social cuja característica é tomar decisões coletivamente vinculantes (LUHMANN, 1992).

Se, entretanto, essas organizações têm como característica a disseminação de suas atividades ao redor do globo, sem uma delimitação territorial específica,

questiona-se o modo como o Sistema da Política, que tem sua estrutura vinculada territorialmente ao Estado, alcançaria esse poder regulamentar.

Na concepção de Vesting (2022, p. 185), faz-se necessária a presença de uma nova percepção de Estado, que não atua tão somente como um ente encarregado de influenciar decisões por meio de mecanismos sancionadores, mas que é observado primordialmente como um mediador das atividades sociais.

Assim, o “Estado em Rede” deve não apenas perceber os novos problemas sociais advindos das atividades prestadas pelas organizações espontâneas, como também estar inserido em um novo contexto de regulação direcionada a esse tipo de atividades.

Nesse sentido, a grande problemática voltada às atividades prestadas por organizações espontâneas na atualidade está vinculada à proteção de dados pessoais.

A relevância desta temática restou destacada desde a revelação do caso Cambridge Analytica, em que foram comprovados o tratamento e a coleta de dados pessoais sensíveis de milhões de eleitores, com o intuito de influenciá-las no processo de tomada de decisão em relevantes eventos democráticos, tais como o Referendum do Brexit em 2015 e as Eleições Presidenciais Americanas de 2016 (FORNASIER, 2020, p. 182-185).

Todavia, mesmo antes dos grandes casos midiáticos sobre o tema, e até mesmo da consolidação da internet como um meio de diferenciação das organizações na sociedade mundial, a Organização para a Cooperação e Desenvolvimento Econômico (OCDE) já promovia uma política de governança global voltada à temática Proteção de Dados Pessoais.

Nesse sentido, a Organização, criada em 1961, que conta atualmente com 38 (trinta e oito) países-membros, tratou da problemática “proteção de dados” mediante sua Convenção de nº 38 (trinta e oito), realizada em 28 de janeiro de 1981 (COUNCIL OF EUROPE, 2022).

Em síntese, a Convenção propunha a adoção de legislação e princípios comuns em matéria de proteção de dados pessoais dos países integrantes da Organização, com o intuito de garantir a aplicação dos direitos fundamentais sobre a matéria nos diferentes territórios (COUNCIL OF EUROPE, 2022).

Nesse contexto de governança em matéria de proteção de dados pessoais surgiu o regulamento europeu sobre proteção de dados pessoais (GDPR) no ano de 2016. Trata-se de uma regulamentação que enquadra os países integrantes da União Europeia na política de governança global da Organização para a Cooperação e Desenvolvimento Econômico (OCDE) sobre a matéria.

Em perspectiva do Mercosul, diversos países passaram a criar legislações específicas sobre o tema, com o intuito de seguir as diretrizes emanadas pela Organização. Nesse cenário, destaca-se, no Brasil, a promulgação da Lei Geral sobre Proteção de Dados Pessoais (LGPD) (BRASIL, 2018).

Praticamente elaborada para enquadrar-se na política global da Organização, garantindo a participação dos países do Mercosul nesse contexto, a Lei Brasileira é fortemente influenciada pelo Regulamento Europeu.

Destaca-se, além dos fatores de transnacionalidade e governança já elencados acima, a presença, na legislação, de uma linguagem que congrega elementos de Gestão e Governança, Direito Digital e Segurança da Informação.

Tratando-se de Segurança da Informação, tais elementos já eram recorrentes na Regulamentação Europeia, que insere a problemática do tratamento de dados pessoais em meios “[...] total ou parcialmente automatizados [...]” (art. 2º, *caput*). Esse contexto acaba por direcionar tecnicamente a atuação de um profissional da área de tecnologia da informação na garantia da “[...] a cifragem ou a pseudonimização” (art.6º, alínea e dos dados existentes nos sistemas de cada organização).

Em matéria de Gestão e Governança, a maturidade organizacional é analisada de modo recorrente em um rol de “salvaguardas necessárias” (art. 6), direcionadas ao responsável pelo tratamento de dados ao titular das informações (art. 12), que deve tomar as “medidas adequadas” nas operações de tratamento de dados pessoais. No mesmo sentido, prevê-se a necessidade da tomada de “medidas que forem razoáveis, incluindo de caráter técnico, tendo em consideração a tecnologia disponível e os custos da sua aplicação” (art. 17) tratando-se dos deveres de informação e do direito de exclusão de dados pessoais a ser pleiteado pelo titular (BRASIL, 2018).

Como comprovação do grau de maturidade da organização em relação ao cumprimento dos dispositivos da Regulamentação, é exigível por parte da autoridade fiscalizadora, a apresentação de relatório que comprove a efetivação de “[...] medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade [...]” com o determinado pelo Regulamento Europeu de Proteção de Dados Pessoais (BRASIL, 2018).

Essa comprovação resta vinculada à aplicação de “códigos de conduta” no âmbito interno da Organização, devidamente adequados ao Regulamento, bem como na realização de “procedimentos de certificação” (art. 24) (BRASIL, 2018).

Tratando-se de procedimentos de certificação, a gestão da organização deve estar diretamente atenta ao cumprimento de medidas técnicas emanadas dos “Organismos de certificação” (art. 43), bem como de determinações do Parlamento Europeu e do Conselho, além da aplicação efetiva das normas ISO/IEC (art. 43, B) (BRASIL, 2018).

Em síntese, portanto, os elementos de Direito Digital presentes nos regulamentos acerca da temática proteção de dados pessoais são baseados em uma análise de maturidade das organizações, calcado na verificação da tomada de decisões adequadas no cumprimento da legislação.

Nesse sentido, as obrigações do responsável pelo tratamento de dados pessoais, em hipótese de fiscalização ou verificação de eventual incidente, são analisadas a partir da verificação da tomada de “[...] técnicas mais avançadas, os custos da sua aplicação, e a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos decorrentes do tratamento para os direitos e liberdades das pessoas singulares [...]”, além da aplicação das “[...] medidas técnicas e organizativas para assegurar que, por defeito, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento” (art. 25).

A matéria de Segurança da Informação, portanto, aparece sempre como um pilar basilar para a comprovação da cultura organizacional exigida. Nesse sentido, destaca-se a utilização de categorias técnicas envolvendo a segurança do tratamento de dados pessoais, tanto pelo responsável quanto por eventuais subcontratantes da organização, que devem observar “[...] as técnicas mais

avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos, de probabilidade e gravidade variável, para os direitos e liberdades das pessoas singulares [...]” utilizando-se de “[...] medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco [...]” (art. 32).

Essa exigência também é direcionada aos subcontratantes das organizações, com a obrigação de apresentarem “[...] garantias suficientes de execução de medidas técnicas e organizativas adequadas de uma forma que o tratamento satisfaça os requisitos do presente regulamento e assegure a defesa dos direitos do titular dos dados” (art. 28).

Todos esses elementos, vinculados à aplicação jurídica efetiva do Regulamento em códigos de conduta ou procedimentos de certificação, são acompanhados de processos específicos, que dependem da intervenção de atividades das áreas de Tecnologia e Segurança da Informação, especialmente “[...] pseudonimização e a cifragem dos dados pessoais” (art. 32, A).

Referidos atos buscam a certificação de que as organizações tomaram as medidas necessárias para a mitigação do “Risco”. Trata-se de uma categoria diretamente vinculada ao processo de tomada de decisão no âmbito das organizações, especialmente destacado na perspectiva de uma sociedade globalizada. (LUHMANN, 2005, p. 146). O Termo é referido na avaliação dos impactos (art. 32), bem como nos procedimentos de atenuação de riscos no tratamento de dados (art. 36).

Outra característica das regulamentações acerca do tema “proteção de dados pessoais” é a criação de profissões típicas, voltadas a essa atividade. Nesse quadro insere-se a figura do *Data Protection Officer* (DPO). Trata-se de um profissional que possui conhecimentos básicos acerca das diferentes áreas envolvidas na Regulamentação, encarregado de mediar as atividades envolvidas para o cumprimento das disposições legais, bem como da comunicação com autoridades fiscalizadoras, devendo ser nomeado pela organização em que atua (art. 37) (BRASIL, 2018).

Ressalta-se, além da aplicação das políticas em proteção de dados pessoais nos códigos de conduta das organizações (art. 46, e), a padronização incentivada por

meio da inclusão das “Cláusulas-tipo de proteção de dados” (art. 46, c e d) nos contratos de transferência de dados, além da exigência de procedimentos de certificação em ambos os lados da contratação (art. 46, f) (BRASIL, 2018).

Tais elementos não apenas reforçam a padronização das ações de transferências de dados, incentivando a implementação interna dos processos de adequação, como também colocam as organizações em contato contínuo com as atualizações oriundas de setores especializados da sociedade. Neste caso em específico, as normas ISO reforçam o caráter de hibridismo das regulamentações acerca de fatos típicos da sociedade em rede.

Nesse contexto, o Brasil tem buscado a adoção de diferentes mecanismos para a resolução de problemas típicos da sociedade mediada pela internet. Em tal sentido, destaca-se a promulgação do Marco Civil da Internet (BRASIL, 2014); da Lei de Acesso à Informação (LAI) (BRASIL, 2011); e da Lei do Governo Digital (BRASIL, 2021). Tais regulamentações, ao lado de dispositivos específicos presentes nas já existentes Lei do Cadastro Positivo (BRASIL, 2011); Código de Defesa do Consumidor (BRASIL, 1990) preveem uma série de fatos relevantes juridicamente no ambiente virtual.

Diferenciam-se desses dispositivos as regulamentações acerca da temática “Proteção de Dados Pessoais”, justamente por congregarem, na própria regulamentação, elementos transdisciplinares e híbridos, que vinculam o seu processo de implementação a práticas globais especializadas.

Em termo estruturais, destaca-se a criação de uma Autoridade Nacional de Proteção de Dados (ANPD), caracterizada como autarquia em regime especial, com autonomia para exercer seu poder regulamentar e exercer a fiscalização do cumprimento da Lei Geral de Proteção de Dados (LGPD).

O envolvimento estrutural do País na proteção de dados pessoais restou impulsionado pela elevação do direito à proteção de dados pessoais ao status de direito fundamental, consagrado no artigo 5º da Constituição Federal Brasileira, mediante o advento da Emenda Constitucional nº 115/2022. (BRASIL, 2022).

Assim, nos termos do artigo 5º, inciso LXXIX: “- é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais” (BRASIL, 1988).

Por meio dos exemplos acima verificados é possível vislumbrar o modo como o Estado -agora em rede- elabora um tipo de regulamentação adaptada à realidade das organizações espontâneas, ciente da necessária aproximação intersistêmica entre diferentes áreas do conhecimento.

O Estado em Rede, na perspectiva de Vesting (2022, p. 185), é justamente o Estado que regula, mas que, ao mesmo tempo, é dependente das prestações sociais das organizações reguladas para a continuidade de suas atividades. Em razão disso, há uma aproximação da linguagem estatal em relação à linguagem típica das organizações reguladas, conforme demonstrado acima em relação à Lei Geral de Proteção de Dados (LGPD).

É típico desse tipo de regulação a concessão de autonomia às organizações para a criação de normas internas, com vista a dar cumprimento ao determinado pela legislação estatal.

Trata-se de um fenômeno próximo ao descrito por Teubner (2016, p. 267) como fragmentação constitucional. São pequenos âmbitos de autonomia regulatória dentro das próprias organizações.

Essa circunstância complementa a concepção de Estado em Rede de Vesting (2022, p. 185), aproximando-se de uma definição de Constituição em Rede, com destaque para modelos de eficácia horizontal dos direitos humanos, consoante se demonstrará a seguir.

2 DO ESTADO À CONSTITUIÇÃO EM REDE: O CARÁTER INTERSISTÊMICO DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

A partir das definições demonstradas acima, é perceptível o modo como, em questões típicas de comunicação mediada pela internet, há um encontro entre diferentes tipos de Constituição.

Portanto, é fundamental, ao mesmo tempo, que o Estado crie estruturas tradicionais para fiscalizar e regulamentar atos voltados a um tema impulsionado pela internet – a exemplo da proteção de dados pessoais – com a fundação de uma autarquia em regime especial, bem como com o advento de uma emenda constitucional.

Do mesmo modo, as regulamentações direcionadas a esse tipo de atividade precisam conter elementos adequados ao tipo de atividade produzida no ambiente virtual.

Nesse sentido, ao mesmo tempo em que resta destacada uma concepção de Estado em Rede, que medeia atividades de interesse público realizadas por atores privados -sendo, ao mesmo tempo, dependente dessas atividades, faz-se necessário pensar em um conceito de Constituição em Rede (VESTING, 2022, p. 185).

Tal proposta parte do intuito de efetivar o direito fundamental à proteção de dados pessoais em contextos adaptados à realidade dos novos fenômenos jurídicos ocorridos no âmbito da comunicação em rede.

Essa fundamentação busca elementos no já destacado contexto de fragmentação constitucional destacado por Teubner (2016), em que os diferentes regimes privados –possuidores de dados pessoais, neste caso – detêm uma capacidade “constitucional” de criação de regulações independentes da Constituição do Estado, mas enfatizando, sobretudo, os elementos caracterizadores de um Constitucionalismo Social.

Nessa expressão, evidenciada nos estudos acerca do constitucionalismo na globalização, destacam-se os elementos de um “direito vivo”, que se manifesta em contextos sociais paralelos ao Estado (ERLICH, 1986). Paralelamente, destaca-se a primeira utilização do termo constitucionalismo social, por Sciulli (1992), com destaque para os estudos acerca da produção de normas em composições colegiadas voltadas a ambientes profissionais e organizações. Referidos eventos foram de fundamental importância na superação parcialmente autônoma de normas impostas por regimes autoritários em determinados momentos da história. (TEUBNER, 2016, p. 133).

A esses elementos, somam-se outras concepções de Constituição, de cunho mais sociológico, mas, principalmente, a definição de Kosselleck, segundo a qual a ideia de Constituição prescinde a aplicação dos ditames constitucionais rotineiramente em diferentes ambientes da sociedade, independentemente da atuação do Estado (VESTING, 2022, p. 186).

Nesse sentido, os novos problemas jurídicos, sobretudo oriundos da comunicação que se dissemina tendo a internet como meio, demandam elementos de uma nova Teoria Constitucional.

Sabendo-se, portanto, do ambiente de autonomia das organizações da sociedade mundial, inclusive na criação e aplicação de regras “constitucionais” próprias, bem como desenvolvendo atividades cuja utilização e dependência não estão vinculados apenas ao setor privado, mas também aos setores tradicionais do Sistema da Política, a percepção de um Estado em Rede demanda consideração de uma Constituição em Rede.

A Constituição em Rede pressupõe que a aplicação do direito fundamental à proteção de dados, como exemplo de um fato típico da sociedade mundial mediada pela internet dependa da concessão de autonomia às diferentes organizações, para que apliquem, mediante seus processos internos de governança, os parâmetros estabelecidos minimamente pelo Estado em Rede, enquanto mediador dessas atividades (VESTING, 2022, p. 186).

Em razão disso, a leitura acerca das novas regulamentações sobre esses fatos, tendo como grande exemplo, no Brasil, a Lei Geral de Proteção de Dados (LGPD) congrega elementos voltados às comunicações típicas desses atores, envolvendo, nas regulamentações, além de institutos jurídicos, a verificação contínua acerca da realização de atos de Gestão e de Tecnologia e Segurança da Informação, que demonstrem a aplicação efetiva, no âmbito interno, de processos prévios de adequação à Regulamentação (BRASIL, 2018).

Nesse sentido, há destaque para análises de políticas de Boas Práticas e Governança nas organizações, exigindo-se que haja a utilização de sistemas estruturados de acordo com requisitos básicos de segurança, na efetivação dos princípios gerais definidos na legislação e demais normas regulamentares (art. 49) (BRASIL, 2018).

Destaca-se, nesse âmbito, a adoção da prática do “Relatório de Impacto” (artigo 5º, inciso XVII), podendo ser exigido da organização, como demonstração do cumprimento das diretrizes estabelecidas na legislação (artigo 10, § 3º e artigo 38). (BRASIL, 2018).

As ações envolvendo os processos de adequação nas organizações envolvem uma série de atores, cujos papéis são descritos na própria legislação. Nesse sentido, tem-se a figura dos “Agentes de Tratamento de Dados Pessoais” (Capítulo VI, artigos 37 e seguintes) a exemplo de Controlador, Operador e Encarregado (similar ao DPO – *Data Protection Officer* no Brasil). Referidos atores também constam nominados no artigo 5º da Lei, com menções frequentes no rol de obrigações da legislação. Ademais, esses atores também estão incluídos em um rol de Responsabilidade e Ressarcimento de Danos (seção III do Capítulo VI, artigos 42 e seguintes). Destaca-se, ainda, a previsão de fatos típicos dos negócios jurídicos envolvidos na regulação, a exemplo da transferência internacional de dados (art. 33 da LGPD).

Observa-se, portanto, o modo como a temática “proteção de dados pessoais”, impulsionada por fatores relacionados à sociedade cuja comunicação é mediada pela internet, possui regulamentações que evidenciam um caráter intersistêmico de tratamento, congregando elementos voltados ao cumprimento de atos transdisciplinares nos ditames da própria Lei, envolvendo elementos de Gestão, de Tecnologia e Segurança da Informação, ao lado do Direito.

Esses elementos reforçam cada vez mais um âmbito de análise da eficácia horizontal dos direitos humanos (TEUBNER, 2016, p.40). Tendo como principal exemplo o direito fundamental à proteção de dados pessoais previsto no artigo 5º, inciso LXXIX, da Constituição Federal (BRASIL 1988), é possível observar o modo como a consolidação prévia de políticas e práticas internas voltadas à proteção de dados pessoais é incentivada pela Lei Geral de Proteção de Dados (LGPD).

Nessa relação, diferenciando-se em relação à tradicional observação vertical na eficácia dos direitos humanos, dependendo de atos diretos do Estado para a sua efetivação, trata-se de um exemplo de concessão cada vez maior de autonomia às organizações, que aplicam os direitos humanos, sob a fiscalização do Estado.

Trata-se, portanto, de uma relação típica do Estado em Rede (VESTING, 2022, p. 196).

Considerando-se que a adoção dessas práticas pode ser observada como a formação de pequenas constituições no âmbito das organizações, vinculando os agentes privados à aplicação dos direitos humanos, na linha Teubner (2016, p. 43), é possível sustentar que esse fenômeno caracteriza a existência de uma Constituição

em Rede, representada pela eficácia horizontal da constituição estatal no âmbito interno das constituições de diferentes atores privados.

CONCLUSÕES

Como se viu ao longo do texto, a consolidação de eventos típicos da sociedade mediada pela comunicação digital exige a criação de legislação específica para tratar dos temas emergentes em matéria de proteção dos direitos fundamentais no ambiente virtual.

A título de exemplo desse fenômeno, o presente trabalho teve como objetivos apresentar o contexto de surgimento da Lei Geral de Proteção de Dados (LGPD), destacando sua inclusão em um processo transnacional de regulamentações sobre o tema, impulsionado pela Organização para a Cooperação e Desenvolvimento (OCDE) (COUNCIL OF EUROPE, 1981).

Para tal, com a intenção de destacar a originalidade das regulamentações de fatos típicos da sociedade mediada pela internet, buscou-se, ao longo do trabalho, evidenciar a diferença do tipo de regulamentação existente na Lei Geral de Proteção de Dados (LGPD) em relação às legislações tradicionais.

Desse modo, apresentou-se uma concepção jurídico-constitucional adequada a compreender e efetivar os processos de adequação jurídica privilegiados pela Lei Geral de Proteção de Dados (LGPD), destacando-se, sobretudo, o modo como os direitos fundamentais devem ser aplicados no ambiente virtual.

Nesse sentido, a teoria de base apresentada para observar a problemática partiu da Teoria dos Sistemas Sociais de Luhmann (2016), de modo a destacar o caráter transdisciplinar das referidas leis, destacando-se, sobretudo, a convergência da comunicação jurídica com elementos específicos de outros sistemas sociais presentes na legislação apontada.

Assim, em relação à Lei Geral de Proteção de Dados (LGPD) e seu principal referencial, o Regulamento Europeu Sobre a Proteção de Dados, mostrou-se o modo como há elementos comunicativos típicos das áreas de Tecnologia da Informação e Segurança da Informação dentro da própria Lei Brasileira. Do mesmo modo,

destacou-se o caráter híbrido das normas ISO, cuja observância é exigida na Lei Geral de Proteção de Dados (LGPD).

Portanto, inicialmente, restou caracterizada a sociedade mundial e sistêmica, na perspectiva de Luhmann (2016), com a necessária consideração dos diferentes âmbitos de comunicação que medeiam os fatos sociais na atualidade.

Ao lado dessa concepção, foi apresentada a sociedade mundial mediada pelos atores típicos da sociedade digital, formando o que Thomas Vesting (2022, p. 186) caracteriza como um “Estado em Rede”.

Essa sociedade, consoante tratado ao longo do trabalho, é caracterizada tanto pela necessidade de regulação, por parte do Estado, de fenômenos típicos da internet, como também representa a dependência, por parte do Estado e de demais organizações da sociedade, dos serviços prestados pelas organizações especializadas em atividades da internet.

Desse modo, ao mesmo passo em que o Estado deve limitar as atividades das organizações especializadas em atividades do ambiente virtual, ele é total dependente desses serviços para a continuidade de suas atividades.

Nesse âmbito, consoante restou demonstrado, há o surgimento das chamadas “organizações espontâneas” (VESTING, 2022, p. 186), que desempenham atividades típicas da internet, sequer possuindo elementos tradicionais do ambiente corporativo, a exemplo da própria territorialidade.

Conclui-se, portanto, em observância do referencial teórico apresentado, bem como do exemplo selecionado para análise, ou seja, a Lei Geral de Proteção de Dados Pessoais (LGPD), que a proteção dos direitos fundamentais no ambiente virtual exige não apenas a criação de legislação específica para os fatos tipicamente vinculados à sociedade mediada pela internet, mas, principalmente, uma compreensão transdisciplinar da aplicação dos direitos que constam em referida legislação.

Assim, em relação à Lei Geral de Proteção de Dados (LGPD) é indispensável a atuação prévia das organizações no cumprimento das medidas de caráter transdisciplinar exigidas na Lei, incluindo, sobretudo, a efetivação de boas práticas e de governança, além da emissão contínua de relatórios e da aplicação das normas ISO. Em síntese, destaca-se o trabalho em conjunto dos setores jurídico, de tecnologia da informação e de segurança da informação.

Nessa linha, conclui-se que a efetividade dos direitos fundamentais em relação à proteção de dados pessoais no ambiente virtual caracteriza-se em uma perspectiva de eficácia horizontal (TEUBNER, 2016, p. 40), não dependendo exclusivamente da atuação do Estado, mas, sobretudo, em caráter prévio de aplicação pelas próprias organizações.

Desse modo, a Lei Geral de Proteção de Dados (LGPD) é um exemplo típico de consolidação dos direitos fundamentais em um ambiente de fragmentação constitucional, típico do constitucionalismo social (ROCHA; COSTA, 2018).

A consolidação da necessária análise transdisciplinar da observância de leis típicas de fatos vinculados à sociedade mediada pela internet, a exemplo do caso da Lei Geral de Proteção de Dados (LGPD) apresentada acima, consolida uma visão de aplicação da "Constituição em Rede" (COSTA; MOURA; FÉLIX, 2023), como prática que enfatiza a necessária observância da eficácia horizontal dos direitos fundamentais no âmbito das organizações, com atuação prévia e demonstração contínua das práticas rotineiras aplicadas para a observância de referida legislação.

REFERÊNCIAS

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 02 set. 2022.

BRASIL. **Emenda Constitucional nº 115, de 10 de fevereiro de 2022**. Brasília, DF: Presidência da República, 2022. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm#art1. Acesso em: 02 set. 2022.

BRASIL. **Lei nº 12.414, de 9 de junho de 2011**. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Brasília, DF: Presidência da República, 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm Acesso em: 01 set. 2022.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de

janeiro de 1991; e dá outras providências. Brasília, DF: Presidência da República, 2022. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 01 set. 2022.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 18 nov. 2022.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 21 set. 2022.

BRASIL. **Lei nº 14.129, de 29 de março de 2021**. Dispõe sobre princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública e altera a Lei nº 7.116, de 29 de agosto de 1983, a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), a Lei nº 12.682, de 9 de julho de 2012, e a Lei nº 13.460, de 26 de junho de 2017. Brasília, DF: Presidência da República, 2021. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14129.htm. Acesso em: 01 set. 2022.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF: Presidência da República, 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L8078compilado.htm. Acesso em: 01 set. 2022.

COSTA, Bernardo Leandro Carvalho.; MOURA, Ariel Augusto Lira de; FELIX, Marcel Carlos Lopes. Constituição em Rede: observações Sociológico-Sistêmicas sobre a Proteção de Dados Pessoais. **Revista de Direito, Governança e Novas Tecnologias**, v. 1, p. 42-61, 2023. Disponível em: <https://indexlaw.org/index.php/revistadgnt/article/view/9225/pdf>. Acesso em: 29 abr. 2023.

COUNCIL OF EUROPE. **Convention 108 and Protocols**. 2022. Disponível em: <https://www.coe.int/en/web/data-protection/convention108-and-protocol#:~:text=The%20Convention%20for%20the%20Protection,in%20the%20data%20protection%20field>. Acesso em: 28 abr. 2023.

EHRlich, Eugen. **Fundamentos da sociologia do direito**. Brasília: Universidade de Brasília, 1986.

FORNASIER, Mateus de Oliveira; BECK, Cesar (2020). Cambridge Analytica: Escândalo, Legado e Possíveis Futuros para a Democracia. **Revista Direito em Debate**, 29 (53), 182–195. Disponível em: <https://www.revistas.unijui.edu.br/index.php/revistadireitoemdebate/article/view/10033>. Acesso em: 18 nov. 2022.

LUHMANN, Niklas. **Poder**. Tradução de Martine Creuset de Rezende Martins. 2.ed. Brasília: Editora Universidade de Brasília, 1992.

LUHMANN, Niklas. **Sociologia del riesgo**. México DF: Universidad Iberoamericana, 2006.

MASCAREÑO, Aldo. Netdoms Digitales. Un nuevo actor en América Latina. *In*: TOLEDO, Enrique de la Garza [et al.]; **Nuevos actores y cambio social en América Latina**. Ciudad Autónoma de Buenos Aires: CLACSO, 2022.

ROCHA, Leonel Severo; COSTA, Bernardo Leandro Carvalho Costa. **Constitutionalismo social**: constituição na globalização. Curitiba: Appris, 2018.

SCIULLI, David. **Theory of Societal Constitutionalism**: Foundations of a Non-Marxist Critical. Cambridge: Cambridge United Press, 1991.

TEUBNER, Gunther. Constitucionalismo social: nove variações sobre o tema proposto por David Sciulli. *In*: CAMPOS, Ricardo; BARBOSA, Samuel. (org.). **Teorias contemporâneas do direito**: o direito e as incertezas normativas. Curitiba: Juruá, 2016.

TEUBNER, Gunther. **Fragmentos constitucionais**: constitucionalismo social na globalização. São Paulo: Saraiva, 2016.

UNITED UNION. **General Data Protection Regulation- GDPR**. 2022. Disponível em: <https://gdpr-info.eu/>. Acesso em: 18 nov. 2022.

VESTING, Thomas. **State Theory and the Law**: an Introduction. Massachusetts: Elgar, 2022.

5. IMPARCIALIDADE DO ÓRGÃO JURISDICIONAL: CONCEITO E TRANSFORMAÇÕES NO CONTEXTO DAS NOVAS TECNOLOGIAS

*THE IMPARTIALITY OF THE COURT: CONCEPT AND CHANGES IN THE CONTEXT OF
NEW TECHNOLOGIES*



<https://doi.org/10.36592/9786554600552-05>

Drieli de Quadros Klippel¹

RESUMO

O presente estudo busca analisar, a partir do direito fundamental à imparcialidade do julgador e o avanço das novas tecnologias no processo, o impacto dos vieses comportamentais nas decisões judiciais. Ainda, se é possível e em que medida é possível empregar a inteligência artificial como ferramenta voltada ao proferimento de decisões judiciais mais justas e imparciais, sem que haja presença de vieses comportamentais dos julgadores.

Palavras-chave: Vieses cognitivos. Inteligência artificial. Algoritmos.

ABSTRACT

The present study seeks to analyze, from the fundamental right to impartiality of the judge and the advancement of new technologies in the process, the impact of behavioral biases in judicial decisions. Also, if it is possible, and to what extent is it possible to use artificial intelligence as a tool aimed at rendering fairer and more impartial judicial decisions, without the presence of behavioral biases on the part of the judges.

Keywords: Cognitive biases. artificial intelligence. algorithms.

¹ Mestranda em Direito pela Pontifícia Universidade Católica do Rio Grande do Sul - PUCRS. Especialista em Direito Registral e Notarial pela Faculdade Damásio Educacional. Bacharel em Direito pela Pontifícia Universidade Católica do Rio Grande do Sul - PUCRS. Advogada. E-mail: Drieli.klippel@hotmail.com. Currículo lattes: <http://lattes.cnpq.br/9813376557827841>.

INTRODUÇÃO

A tecnologia, a partir da implementação do processo eletrônico, tornou-se uma ferramenta indispensável nas relações processuais, por diversos motivos, tais como a facilidade de acessar ao poder judiciário, sem a protocolização de forma física, a praticidade processual em audiências, a visualização do processo por meio eletrônico, extinguindo a necessidade de realizar carga do processo para conseguir ter acesso ao conteúdo. Além disso, muitos jurisdicionados procuram e necessitam de um processo com etapas mais céleres. A tecnologia, sem dúvida, auxilia neste aspecto também. A utilização de mecanismos com inteligência artificial, como é o caso da ferramenta *Victor*, utilizada pelo Supremo Tribunal Federal, ou da ferramenta *Athos*, utilizada pelo Superior Tribunal de Justiça, alcança resultados efetivos em um lapso temporal curto, comparado com um humano, no desempenho de tarefas repetitivas.

No entanto, abrindo o leque de utilidades desses mecanismos, e partindo da premissa de desenvolvimento de um algoritmo que proferirá decisões judiciais, é necessário lançar luz na utilização desses agentes e nos riscos ligados às informações enviesadas que podem surgir no proferimento de uma decisão.

Nesse âmbito, o pressuposto teórico principal que norteia este estudo é que a utilização da inteligência artificial no proferimento de decisões judiciais não poderá apenas funcionar como um desafogamento do judiciário, sem levar em conta os impactos negativos que podem ser gerados, ocasionando violação ao princípio constitucional e garantia processual à imparcialidade do julgador.

A pesquisa aponta alguns pontos sobre o direito fundamental e garantia processual à imparcialidade do julgador, sob o primado das novas tecnologias, a partir dos seguintes problemas: a) Qual a origem e conceituação do direito fundamental à imparcialidade do juiz e seu alcance no processo civil brasileiro? b) De qual maneira a utilização de ferramentas de inteligência artificial garantem imparcialidade no âmbito processual? Quais os entraves? Quais os limites?

A metodologia de abordagem utilizada na presente pesquisa é essencialmente a hipotético-dedutiva, na medida em que se pretende confirmar ou refutar a hipótese provisória de que o emprego de inteligência artificial em decisões

judiciais pode contribuir com um processo mais imparcial, eis que está livre dos vieses cognitivos dos julgadores.

O trabalho se desenvolverá através do método histórico, ao analisar o conceito de imparcialidade e a construção constitucional deste princípio. Ainda, o método monográfico realizará estudo sobre a imparcialidade do órgão jurisdicional, de acordo com o entendimento da doutrina e das previsões existentes nos tratados internacionais de direitos humanos que o Brasil é signatário. Também se utilizará do método funcionalista, porque se pretende analisar a aplicabilidade de ferramentas com inteligência artificial no processo e o cumprimento da garantia processual à imparcialidade, frente aos vieses subjetivos.

O objetivo da presente pesquisa não é fazer oposição ao uso de agentes com inteligência artificial, mas expandir o debate, especialmente entre pesquisadores de múltiplas áreas, estimulando a discussão sobre o tema e apontando obscuridades que precisam ser esclarecidas.

1 AS DIRETRIZES DA CONSTITUIÇÃO FEDERAL E DO CÓDIGO DE PROCESSO CIVIL ACERCA DA IMPARCIALIDADE DOS JULGADORES

O direito fundamental das partes à imparcialidade do juiz, embora não seja um direito fundamental expresso no art. 5º da Constituição Federal é encontrado em diversos Tratados Internacionais de Direitos Humanos, em que o Brasil é signatário, tais como o art. 10 da Declaração Universal dos Direitos Humanos e o art. 14 do Pacto Internacional sobre Direitos Civis e Políticos, entre outros. O conteúdo do julgamento por um julgador imparcial existe em decorrência de uma leitura sistemática da Constituição. A imparcialidade é encontrada de forma implícita na Constituição, eis que o §2 do art. 5º não exclui outros direitos fundamentais decorrentes dos tratados internacionais em que a República Federativa do Brasil seja signatária. Portanto, além de uma garantia processual, a imparcialidade dos julgadores encontra proteção constitucional.

Além de um direito fundamental, o dever de imparcialidade do julgador encontra previsão nos artigos 144 e 145 do Código de Processo Civil. Os referidos artigos trazem as causas de impedimento e de suspeição do juiz. Ou seja, opera as

hipóteses em que o magistrado não deve atuar, sob pena de ferir a garantia processual à imparcialidade.

A ideia de imparcialidade, de acordo com Antônio do Passo Cabral (CABRAL, 2007, p. 02) está atrelada à “ausência de interesse judicial na sorte de qualquer das partes quanto ao resultado do processo”. Outra linha possível na busca do significado da ideia de imparcialidade do juiz é definir a imparcialidade a partir da anotação de traços que não podem estar presentes na atuação jurisdicional, tratando-a como “a ausência de qualquer ‘interesse pessoal’ ou ‘envolvimento emocional’ do julgador com o feito”, como uma “virtude passiva” da jurisdição (OLIVEIRA, MITIDIERO *apud*, REICHELT, 2014, p. 02).

A presente ideia aborda uma visão de cunho “negativo” por parte do juiz, uma espécie de abstenção do julgador (SARLET, 2018, p. 46). Assim, de acordo com as teorias das dimensões dos direitos fundamentais, a imparcialidade, sob este aspecto, pode ser entendida como direito fundamental de primeira dimensão.

A imparcialidade, ainda, pode ser explorada a partir do dever de adoção de certa conduta por parte do julgador (REICHELT, 2014, p. 02). Aqui a imparcialidade está relacionada ao dever e garantia de um agir com imparcialidade na solução da causa que lhe é submetida. Prevalece a ideia de cunho “positivo” (SARLET, 2018, p. 47) do julgador, podendo ser considerada, portanto, um direito fundamental de segunda dimensão.

Segundo Reichelt (REICHELT, 2014, p. 03), haverá quebra da imparcialidade do juiz toda vez que o seu agir no processo for movido por outra razão que, de alguma forma, indique a presença de confusão entre as razões que o levaram a proferir a decisão judicial em determinado sentido e o interesse que move às partes no debate dos autos. E continua, o interesse que deve mover o julgador ao proferir decisões é o de aplicar ao caso concreto o estabelecido pelo ordenamento jurídico.

O autor Alvarado Velloso (VELLOSO, 2014. p 207-235) aborda inúmeros atos que o julgador deve manter, a fim de garantir às partes um julgamento livre de qualquer parcialidade. E assim diz, “que o julgador deve estar livre de preconceitos de qualquer tipo”, incluindo, sem se limitar, aos raciais e aos religiosos. Ainda, deve haver independência de qualquer opinião, ou seja, “não estar sob influência de qualquer opinião ou persuasão das partes”. Não deve se identificar com qualquer

ideologia elucidada. Manter-se alheio a qualquer suborno, amizade, inimizade, ódio, sentimento de caridade, preguiça, desejos de brilho pessoal, entre outros.

Por outro lado, a imparcialidade do juiz pode ser vista como consequência lógica do princípio do juiz natural, princípio fundamental que carrega a substância da jurisdição (THEODORO JR, 2015, p. 180). Assim, há de se entender o dever de imparcialidade como componente indispensável à existência do devido processo legal. Este, que se justifica por sua legalidade e legitimidade, jamais comportaria em sua essência o julgamento por um juiz parcial, que decide a partir de seus próprios interesses ao arrepio da lei (THEODORO JR, 2015, p. 98).

Mesmo com todo o cuidado do julgador para não estar sujeito a situações que possam enviesar uma decisão, existem subterfúgios que são alheios à sua vontade. Como é cediço, o pensamento humano ao proferir uma decisão pode levar em conta diversos vieses subjetivos, que fogem do cenário imparcial a que o juiz está submetido. As simplificações mentais, embora na maioria das vezes funcionem com sucesso e atendam às necessidades primárias humanas (THALER, SUNSTEIN, 2019, p. 27-51), há casos em que o recurso a atalhos mentais acabam por prejudicar o processo decisório, como a heurística comportamental (MORAES, TABAK, 2018, p. 629).

O cenário atual, em que o uso da inteligência artificial está cada vez mais em voga ao âmbito processual, é rodeado por dúvidas e anseios quanto à imparcialidade do órgão jurisdicional que se utiliza da inteligência artificial, na medida em que não há garantias de que os sistemas utilizados estejam totalmente livre de opiniões e preconceitos intrínsecos de seus fundadores. Além disso, o enviesamento pode estar presente no abastecimento de dados que já estejam enviesados, que conseqüentemente proferirá outras decisões enviesadas. É preciso que os obstáculos sejam superados, ou ao menos, explicados, sob pena de causar insegurança jurídica aos jurisdicionados e descredibilidade do poder judiciário.

2 INTELIGÊNCIA ARTIFICIAL E OS VIESES SUBJETIVOS DOS JULGADORES

A inteligência artificial, de forma sucinta, pode ser compreendida como capacidade que as máquinas têm de, desde que dotadas de conjuntos de algoritmos

corretos, emular o comportamento humano (TURING, 1950, p. 60-433). Para Jordi Nieva Fenoll (FENOLL, 2018, p. 20), inteligência artificial é a capacidade de máquinas pensarem ou imitarem o pensamento humano, até certo ponto. Da mesma forma, outra alternativa sobre conceito de inteligência artificial é a trazida pelos autores Stuart Russell e Peter Norwig (RUSSEL, NORWING, 2010, p. 01-04) os quais entendem que é a construção de agentes com racionalidade, ou seja, aqueles que agem e pensam de modo a atingir o melhor resultado que se possa esperar, de maneira racional.

Partindo para a doutrina nacional, Denise Fincato e Cecília Silva (FINCATO, SILVA, 2019, p. 2) trazem a inteligência artificial como "um ramo da ciência da computação em que as máquinas podem aprender, pensar, agir e adaptar-se ao mundo real, ampliando e simulando a capacidade humana, automatizando tarefas e ajudando a solucionar alguns dos problemas sociais mais desafiadores".

A inteligência artificial, com base nos conceitos apresentados, será analisada sob o prisma do proferimento de decisões. Ou seja, as decisões serão proferidas por mecanismos de inteligência artificial e não mais por um juiz humano.

É vantajoso em alguns aspectos recorrer-se ao uso da inteligência artificial. Em 2018 o Supremo Tribunal Federal anunciou o programa de inteligência artificial chamado de *Victor*. O programa identifica vinculações aos temas de repercussão geral, com o objetivo de aumentar a velocidade de tramitação (NUNES, MARQUES, 2018, p. 02). O presente mecanismo apresentou um ganho temporal surpreendente em suas atividades. Tarefas que eram realizadas por mãos humanas não possuíam tanta agilidade e assertividade em suas conclusões, quanto às tarefas desempenhadas por *Victor*. As etapas processuais no Supremo Tribunal Federal ganharam um novo rumo, sob o aspecto da celeridade processual.

Os robôs *Alice*, *Sofia* e *Mônica* vêm sendo empregados pelo Tribunal de Contas da União para examinarem os editais de licitações, buscando possíveis fraudes ou irregularidades, além de acompanhar as compras públicas (FERRARI, BECKER WOLKART, 2018, p. 02). Tendo em vista o sucesso dos mecanismos, os robôs já estão sendo utilizados em outros órgãos, como no Ministério Público, Tribunais de contas estaduais, entre outros.

O desenvolvimento tecnológico proporciona um cenário em que a utilização de mecanismos com inteligência artificial está cada vez mais em voga. Em outros ambientes a utilização de mecanismos de inteligências artificiais são cada vez mais usuais. Por exemplo, a análise de crédito feita por instituições financeiras, recomendações de músicas nas plataformas digitais, sugestão de amigos nas redes sociais, sugestões de consumo e diversas outras atividades que, muitas vezes, sequer percebemos.

Os sistemas de Inteligência Artificial trazem benefícios ao ambiente processual, especialmente em relação à automatização de atividades repetitivas, proporcionando maior agilidade e celeridade nas etapas processuais e maior precisão em sua realização. Com a utilização desses agentes, tarefas que demandam um tempo razoável para conclusão, são finalizadas em poucos segundos.

No entanto, é preciso que a utilização desses sistemas seja exaurida de forma mais aprofundada. Não basta apenas considerar os ganhos de eficiência e produtividade. Os jurisdicionados devem estar amparados por sistemas que cumpram as diretrizes do devido processo legal, sob pena das tecnologias utilizadas serem consideradas insuficientes, ou até mesmo contrárias aos ditames constitucionais.

A inserção de mecanismos tecnológicos no Direito brasileiro dificilmente retrocede. O maior exemplo disso foi a inserção do processo eletrônico. Inicialmente, foi implementado em algumas situações pontuais, como na interposição de recursos de agravo de instrumento e demandas vinculadas aos juizados especiais. Hoje, os processos físicos caminham à beira da extinção. A evolução caminha em passos rápidos, principalmente, a evolução tecnológica. Isto é um fato.

O uso da tecnologia pode trazer diversos benefícios para o sistema. No entanto, é imprescindível que se tenha cuidado em sua implementação, e principalmente, nas atividades realizadas por estes programas. O uso de algoritmos apresenta riscos não evidentes, que podem surgir tanto no momento de elaboração dos algoritmos enviesados, pelo seu próprio programador, quanto no abastecimento de dados enviesados.

Um caso emblemático envolvendo inteligência artificial e vieses, que gerou um grande debate, foi o episódio envolvendo o emprego do sistema Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) para fins de cálculo do risco de reincidência de uma pessoa presa (REICHELDT, 2021, p. 05). O algoritmo acabava privilegiando encarcerados brancos e estabelecendo um índice de reincidência mais alto aos encarcerados negros.

As decisões judiciais, assim como visto no caso COMPAS, podem estar atreladas a muitos vieses subjetivos de seus julgadores, causando prejuízos infundados aos jurisdicionados, baseados em crenças, ideologias, preconceitos, visões distorcidas da realidade, entre outros. A utilização de meios tecnológicos, como a inteligência artificial, seria uma forma de inibir os problemas relacionados à imparcialidade do julgador. A retirada de um julgador humano, que está atrelado em sua natureza às simplificações e aos vieses comportamentais no momento da tomada de decisões, poderia, sem dúvida, conceder um processo mais igualitário entre as partes. Ocorre que, no mundo real, não existe quem esteja inteiramente imune a automatismos mentais, cujo mapeamento revela-se, portanto, de extrema utilidade (FREITAS, 2013, p. 224).

Daniel Kahneman (KAHNEMAN, 2012, p. 13) prevê a existência de dois sistemas de pensamento, no campo da interpretação jurídica: o sistema I (pensamento automático) e o sistema II (controle racional). E continua, o sistema I opera automática e rapidamente, tomando a maior parte das decisões por impulso, sem maior senso de controle voluntário. O sistema II diz respeito àquelas áreas do cérebro mais novas, responsáveis pelo esforço de calcular, pela concentração, pelo monitoramento e controle das sugestões formuladas pelo sistema I.

O que o autor buscou destacar, foi que o sistema automático (sistema I) é uma verdadeira usina de enviesamentos, distorções e erros em cascata, longe do abrigo seguro da prudência, incorrendo em inconsistências e ilusões de controle (FREITAS, 2013, p. 228).

Segundo Juarez Freitas (FREITAS, 2013, p. 224), todo cérebro humano ostenta desvios cognitivos que, não raro, afetam negativamente a qualidade da interpretação. Ocorre que, no mundo real, não existe quem esteja inteiramente imune a automatismos mentais. É inerente à natureza humana.

Um grande balizador dos vieses subjetivos dos julgadores, é que nenhum juiz gosta de admitir que pode estar influenciado por vieses ou ilusões cognitivas. Mesmo com grandes estudos sobre o tema, que comprovam a existência e a interferência dos vieses nas decisões judiciais, o assunto ainda se encontra nebuloso no meio da tomada de decisões.

Ainda, os sistemas de inteligência artificial empregados também podem ser parciais, além de estarem impregnados de juízos de valor, opiniões pessoais tomadas de emoção e sentimentos daqueles que programaram seus dados. O enviesamento, inclusive, pode ser no momento da elaboração pelo próprio programador (CANTALI, ENGELMANN, 2021, p. 44).

Assim, há de se perceber a necessidade de analisar e definir com segurança o conteúdo dos algoritmos empregados, de modo a fornecer um processo decisório imparcial, justo e de acordo com as diretrizes da Constituição Federal, evitando que ocorra a perpetuação das desigualdades sociais, raciais, erros e outras mazelas de nossa sociedade, por meio de vieses algorítmicos. É preciso contornar os obstáculos com acessibilidade e transparência na tomada de decisão.

3 A UTILIZAÇÃO DOS ALGORITMOS NA TOMADA DE DECISÕES E SUA CONSTRUÇÃO

É possível encontrar diversas instituições no Brasil, públicas e privadas, valendo-se da inteligência artificial. Por esse motivo é importante refletir sobre algumas premissas para assegurar que, uma vez que a inteligência artificial seja implementada, não como simples auxílio, mas para tomada de decisões automatizadas pelo Poder Judiciário, tal providência não implique em violação às garantias fundamentais do processo, em especial à imparcialidade do órgão jurisdicional (CANTALI, ENGELMANN, 2021, p. 67).

Ocorre que os algoritmos empregados, ao proferimento de decisões judiciais, também podem estar sujeitos ao enviesamento e acabar reproduzindo justamente o comportamento humano que deveriam evitar. Antes de adentrar ao assunto principal, é necessário fazer uma breve síntese do que é, e de como são classificados os algoritmos.

Não há unanimidade no conceito de algoritmo. No presente estudo, será considerada a definição trazida por Pedro Domingos, que sustenta: “algoritmo é uma sequência de instruções que diz a um computador o que fazer” (DOMINGOS, 2015, p. 01).

Além disso, os algoritmos podem ser classificados em dois tipos: programados ou não programados. Algoritmos programados seguem as diretrizes estabelecidas pelo programador. Ou seja, os dados entram no sistema, o algoritmo compatibiliza as informações e o resultado sai do sistema, com os dados já processados (FERRARI, BECKER, WOLKART, 2018, p. 04).

A estrutura algorítmica não programada ou não supervisionada, ao contrário, trabalha a partir de dados não programados, apenas abastecidos, deixando que o próprio mecanismo encontre padrões, sem que exista uma predefinição (CANTALI, ENGELMANN, 2021, p. 50). O presente estudo não examinará as peculiaridades e diferenças de cada tipo de algoritmos. Estes poderiam gerar, por si só, um artigo.

Os autores (FERRARI, BECKER, WOLKART, 2018, p. 03) sustentam que a utilização de algoritmos, programados ou não programados, pode apresentar riscos não evidentes, tais como: “(i) de *data sets* viciados; (ii) da opacidade na sua forma de atuação, consequência das técnicas de *machine e deep learning*; (iii) da possibilidade de promoverem a discriminação ainda que bem estruturados”.

É preciso que os algoritmos utilizados cumpram alguns critérios, tais como: fundamentação nas decisões judiciais proferidas, transparência dos algoritmos, ou seja, devem publicizar os parâmetros que levaram ao proferimento de determinada decisão e a construção dos algoritmos conjuntamente com a comunidade jurídica.

Uma decisão judicial que não tenha uma fundamentação coerente, exaurida e aplicável ao caso em questão, ocasiona vários vícios ao processo. Aliás, sem os fundamentos da decisão judicial, além da violação do dever de fundamentação, imposto pela Constituição Federal, acaba comprometendo o direito de defesa, já que não há como recorrer de uma decisão que não os apresenta (CANTALI, ENGELMANN, 2021, p. 40).

Assim, a fundamentação na tomada de decisões deve sempre estar presente, seja a decisão proferida por um juiz humano, ou por um sistema de inteligência artificial, sob pena de ferimento a diversos princípios e garantias constitucionais.

Além disso, a autora Isabela Ferrari (FERRARI, 2019, p. 10) sustenta que deve haver transparência na forma de discussão e estruturação desses programas. Só assim se poderá determinar os softwares passíveis de utilização pelo Poder Judiciário, garantindo que tenham uma estrutura menos opaca, além de permitir uma explicabilidade efetiva (CANTALI, ENGELMANN, 2021, p. 10).

A construção dos mecanismos deve se dar conjuntamente entre juristas e cientistas (FERRARI, BECKER, WOLKART, 2018, p. 03). E mais, no que tange aos juristas é necessário a participação não só dos magistrados, mas da comunidade jurídica como um todo, por exemplo, com representantes também da Ordem dos Advogados e de outros órgãos relacionados, como o Ministério Público e profissionais de áreas correlatas, especialmente, vinculadas à tecnologia.

Além da seleção dos dados e construção dos algoritmos, é imprescindível atentar-se ao impacto que o posicionamento da decisão irá refletir. Decisões são questionáveis, nenhum caso é igual ao outro. A automatização das decisões pode gerar um problema de congelamento de decisões e com isso tornar assuntos importantes imutáveis.

Para Pinto, a realização de auditoria nos algoritmos utilizados, torna-se bastante complexo. Não se quer dizer que um monitoramento viável e adequado seja algo impossível, mas até agora pouco se fala a respeito de um software inteligente capaz de compreender as múltiplas linguagens traduzidas para esses sistemas, voltadas ao exame de eventuais vieses que podem ter sido captados pelas máquinas e que acabam repetindo os preconceitos existentes (PINTO, 2020, p. 56).

O autor acima referido complementa, ainda, que as sociedades do futuro correrão sério risco de se submeterem a um rápido e intenso processo, que utilize algoritmos (*machine learning*), caso o debate ético e antropológico não seja efetivamente realizado e aprofundado por governos, sociedade civil, setores empresariais, organizações nacionais e internacionais (PINTO, 2020, p. 58).

Nesse contexto, há que tratar-se, igualmente, da normatização específica de matérias relativas à inteligência artificial e robôs, eis que o ordenamento jurídico existente não abrange de forma completa estes assuntos. Institutos como o da responsabilidade civil é de suma importância ser exaurido, para lidar com os novos conflitos oriundos da relação humano e máquina (TEFFÉ, MEDON, 2020, p. 303).

Em contraponto, ao tratar da utilização de algoritmos para fins de melhorar o processo decisório, Ana Frazão afirma que a exploração de algoritmos para tal fim é a de substituir as decisões humanas, consideradas naturalmente falhas e enviesadas, pelas escolhas algorítmicas, vistas como mais eficientes, objetivas e imparciais (FRAZÃO, 2018, p. 309).

A autora aborda a hipótese de agentes que se utilizam de inteligência artificial e que acabam transferindo a responsabilidade de decidir às máquinas, não mais responsabiliam pelo que estas fizessem. De alguma maneira, há que se pensar na responsabilidade dos agentes empresariais pelas tecnologias que adotam e por meio das quais auferem lucros e proveitos (FRAZÃO, 2018, p.4).

Por outro lado, a responsabilidade decisória em um processo judicial cabe ao prolator da decisão, ou seja, ao juiz responsável para tal função de forma subjetiva, e de forma objetiva, ao Estado que outorgou a atividade ao agente.

É fundamental que possamos avançar nessas reflexões, a fim de encontrar uma justa medida para equilibrar inovação e responsabilidade, assim como evitar a indesejável "irresponsabilidade organizada" por parte das empresas criadoras e gestoras das máquinas (FRAZÃO, 2018, p. 06).

A utilização de inteligência artificial é, sem dúvida, uma alternativa viável e necessária para a obtenção de um processo mais célere e muitas vezes mais efetivo. Além disso, apresenta um caráter econômico estatal, na medida que determinadas tarefas, que antes eram desempenhadas por várias pessoas, hoje são simplificadas apenas com a utilização de sistemas inteligentes.

Ocorre que é preciso analisar, no âmbito de tomada de decisões, a elaboração, construção dos sistemas, e principalmente a aplicação dos algoritmos ao caso concreto. De nada adianta criar um algoritmo extremamente avançado, se os dados que o alimentam são enviesados. Os autores Teffé e Medon dão como exemplo de dados enviesados, o exemplo da Inteligência artificial desenvolvida pela Microsoft, Tay, que realizou no Twitter declarações racistas, antissemitas, sexistas, conspiratórias e revisionistas, as quais poderiam até mesmo ser qualificadas penalmente como injúrias raciais, crimes de incitação ao ódio e discriminação racial (TEFFÉ, MEDON, 2020, p. 310).

É importante refletir sobre as consequências do uso da inteligência artificial e das suas repercussões. Afinal, caso as coisas não saiam bem como o imaginado, de quem será a responsabilidade? É fundamental questionar, assim, se é esse o objetivo que esperamos encontrar nas inovações (SANTOS, CRESPO, 2017, p. 01).

Assim, percebe-se, que há grande chances de decisões proferidas por agentes com inteligência artificial violarem direitos fundamentais, sem os devidos cuidados éticos, constitucionais, que cumpram integralmente a transparência, gestão, motivação e imparcialidade no proferimento de decisões.

CONCLUSÃO

O presente estudo buscou analisar o direito fundamental e garantia processual à imparcialidade do julgador, frente aos vieses subjetivos que interferem na atividade jurisdicional, considerando a utilização de sistemas com inteligência artificial.

São diversas as motivações implícitas tocantes às decisões judiciais, que acabam por incentivar o uso da discricionariedade e do decisionismo, tornando a decisão dos magistrados parciais e fora dos ditames estabelecidos pela Constituição Federal. Até mesmo os sistemas dotados de inteligência artificial, em um cenário de tomada de decisões, estão rodeados por subjetividades, eis que os dados que abastecem os agentes podem estar corrompidos por decisões enviesadas e que acabam proferindo mais decisões fora dos padrões constitucionais, gerando assim uma verdadeira indústria de enviesamentos.

Não há garantia de que os mecanismos utilizados estejam livres dos vieses subjetivos de seus criadores e programadores, ou até mesmo dos dados anexados.

Assim, é preciso que alguns requisitos sejam obedecidos, na elaboração e no proferimento de decisões, quando se tratar de agentes com inteligência artificial, tais como: fundamentação nas decisões judiciais proferidas, transparência dos algoritmos e a construção dos algoritmos conjuntamente com a comunidade jurídica.

O presente estudo está longe de encontrar a solução para o problema apresentado, que pode estar, efetivamente, ou não nas soluções apresentadas. A

intenção final é sugerir formas que possam auxiliar em uma tomada de decisão mais justa, transparente e que atinja, em parte, as diretrizes do devido processo legal.

REFERÊNCIAS BIBLIOGRÁFICAS

CABRAL, Antônio do Passo. Imparcialidade e imparcialidade: por uma teoria sobre repartição e incompatibilidade de funções nos processos civil e penal. **RePro**, 2007, p. 149/341.

CANTALI, Fernanda Borghetti. ENGELMANN, Wilson. Do não cognitivismo dos homens ao não cognitivismo das máquinas: percursos para o uso de decisões judiciais automatizadas. **Revista Jurídica Portucalense**, n. 29, 2021.

DOMINGOS, Pedro. **The master algorithm**: how the quest for the ultimate machine learning will remake our world. Nova York: Basic Books, 2015.

FERRARI, Isabela. Accountability de Algoritmos: a falácia do acesso ao código e caminhos para uma explicabilidade efetiva. **ITS Rio**, 2019.

FERRARI, Isabela; BECKER, Daniel. WOLKART, Erik Navarro. Arbitrium ex machina: panorama, riscos e a necessidade de regulação das decisões informadas por algoritmos. **Revista dos Tribunais Online**, 2018.

FINCATO, Denise Pires; SILVA, Cecília Alberto Coutinho. Automação, inteligência artificial e futuro da advocacia: empregabilidade como um direito. **Revista de Direito e as Novas Tecnologias**. São Paulo, v. 2, 2019.

FRAZÃO, Ana. FRAZÃO. Algoritmos e inteligência artificial. **Jota**, v. 15, 2018.

FREITAS, Juarez. A hermenêutica jurídica e a ciência do cérebro: como lidar com os automatismos mentais. **Revista da AJURIS**, v. 40, n. 130, 2013.

KAHNEMAN, Daniel. **Thinking, Fast and Slow**. London: Penguin Books, 2012.

MORAES, José Diniz de; TABAK, Benjamin Miranda. As heurísticas e vieses da decisão judicial: análise econômico-comportamental do direito. **Revista Direito GV**. vol. 14, n. 2, 2018.

NUNES, Dierle. MARQUES, Ana Luiza Pinto Coelho. Inteligência artificial e direito processual: vieses algorítmicos e os riscos de atribuição de função decisória às máquinas. **Revista de Processo**. 2018.

OLIVEIRA, Carlos Alberto Álvaro de; MITIDIERO, Daniel. Curso de processo civil, apud REICHELDT, Luis Alberto. O direito fundamental das partes à imparcialidade do juiz no direito processual civil. **Revista de processo**, v. 227, 2014.

PINTO, Henrique Alves. A utilização da inteligência artificial no processo de tomada de decisões: por uma necessária *accountability*. **Revista de Informação Legislativa**: RIL, Brasília, DF, v. 57, n. 225, p. 43-60, 2020.

REICHELDT, Luís Alberto. O direito fundamental das partes à imparcialidade do juiz no direito processual civil. **Revista de processo**, v. 227, 2014.

REICHELDT, Luís Alberto. Inteligência artificial e direitos fundamentais processuais no âmbito cível: uma primeira aproximação. **Revista de Processo**. São Paulo, v. 312, 2021.

ROQUE, André Vasconcelos. SANTOS, Lucas Braz dos Rodrigues. Inteligência artificial na tomada de decisões judiciais: três premissas básicas. **Revista Eletrônica de Direito Processual**, v. 22, n. 1, 2021.

SANTOS, Coriolano Aurélio de Almeida Camargo. CRESPO, Marcelo. Inteligência artificial, algoritmos e decisões injustas: é hora de revermos criticamente nosso papel em face da tecnologia. **Migalhas**, 2017.

SARLET, Ingo. **A eficácia dos direitos fundamentais**: uma teoria geral dos direitos fundamentais na perspectiva constitucional. 13 ed. Porto Alegre, Livraria do Advogado, 2018.

TEFFÉ, Chiara Spadaccini. MEDON, Filipe. Responsabilidade Civil e Regulação de novas tecnologias: Questões acerca da utilização de inteligência artificial na tomada de decisões empresariais. **Revista Estudos Institucionais**, 2020, v. 6, n. 1.

THEODORO JR., Humberto. **Curso de Direito Processual Civil** – Teoria geral do direito processual civil e processo de conhecimento – Volume I. Rio de Janeiro: Forense, 2015.

THALER, Richard H. SUNSTEIN, Cass R. **Nudge**: Como tomar melhores decisões sobre saúde, dinheiro e felicidade. Tradução Ângelo Lessa, 1ª ed., Rio de Janeiro, 2019.

TURNING, A. M. Computing machinery and intelligence. **Mind**. v. 59, n. 236, 1950.

VELLOSO, Adolfo Alvarado. La imparcialidad judicial y el debido proceso. **Revista Ratio Juris**. v. 9, n. 18, 2014.

6. O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS E A ESTRATÉGIA DE SAÚDE DIGITAL PARA O BRASIL: ANÁLISE DA APLICAÇÃO DA LGPD NO TRATAMENTO DE DADOS PESSOAIS NO SISTEMA E-SAÚDE

FUNDAMENTAL RIGHT TO PROTECT PERSONAL DATA AND THE DIGITAL HEALTH STRATEGY FOR BRAZIL: ANALYSIS OF THE APPLICATION OF LGPD IN THE PROCESSING OF PERSONAL DATA IN THE E-HEALTH SYSTEM



<https://doi.org/10.36592/9786554600552-06>

Emmanuel Rocha Reis¹

Ricardo Luís Lenz Tatsch²

RESUMO

O presente trabalho apresenta a temática do tratamento de dados pessoais sensíveis na política nacional da saúde digital, considerando a visão da Estratégia de Saúde Digital (ESD28), para o Brasil, que compreende a sistematização e consolidação da saúde digital nacional, com os anos de 2020 a 2028 como marco de sua aplicação. Assim, apresenta-se a problemática do tratamento de dados pessoais sensíveis na política nacional da saúde digital e possíveis limites no seu uso, considerando a diversidade de atores e dos interesses das organizações presentes no complexo processo da saúde brasileira, apresentando interseções da LGPD diante das fragilidades do sistema e buscando um parâmetro limitador para o uso desses dados. Dessa forma, a partir do método procedimental dogmático, de caráter descritivo, com levantamento bibliográfico e documental, utilizando dados do Ministério da Saúde, periódicos, legislações etc., apresenta-se resultados parciais sobre a possível identificação de limites no uso de dados pessoais sensíveis na

¹ Mestre em Direito pela Universidade Federal do Piauí – UFPI. Doutorando em Direito - PPGDPUCRS, Bolsista CAPES/PROEX. Participante do Grupo de Estudos e Pesquisa em Direitos Fundamentais (PUCRS). Advogado e Professor do Curso de Direito da UESPI. Currículo Lattes: <http://lattes.cnpq.br/0173325731450357>. E-mail: emmanuel.reis@edu.pucrs.br.

² Mestre e doutorando em Direito pela Pontifícia Universidade Católica do Rio Grande do Sul – PUCRS. Participante do Grupo de Estudos e Pesquisa em Direitos Fundamentais (PUCRS). Procurador Regional da República. Currículo Lattes: <http://lattes.cnpq.br/3162417730641494>. E-mail: ricardo.tatsch@edu.pucrs.br.

política nacional da saúde digital, considerando a dinâmica de transmissão de dados entre sistema público e privado de saúde.

Palavras-chave: Estratégia de saúde digital. Tratamento de dados. Dados sensíveis. LGPD.

ABSTRACT

The present work presents the theme of the treatment of sensitive personal data in the national digital health policy, considering the vision of the Digital Health Strategy (ESD28), for Brazil, which comprises the systematization and consolidation of the national digital health, with the years 2020 to 2028 as the milestone of its application. Thus, the problem of processing sensitive personal data in the national digital health policy and possible limits on its use are presented, considering the diversity of actors and interests of organizations present in the complex process of Brazilian health, presenting intersections of the LGPD in the face of the weaknesses of the system and seeking a limiting parameter for the use of these data. Thus, based on the dogmatic procedural method, of a descriptive nature, with a bibliographical and documentary survey, using data from the Ministry of Health, journals, legislation etc., partial results are presented on the possible identification of limits in the use of personal data sensitive data in the national digital health policy, considering the dynamics of data transmission between the public and private health systems.

Keywords: Digital health strategy. Data processing. Sensitive data. LGPD.

1 INTRODUÇÃO

O percurso do trabalho desenvolverá a temática do tratamento de dados pessoais sensíveis na política nacional da saúde digital, diante da análise de limites do uso, considerando diretrizes da Lei nº 13.079, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados – LGPD), com a redação dada pela Lei nº 13.853/2019, diante da visão da Estratégia de Saúde Digital (ESD28)³, para o Brasil, que compreende a

³ A ESD28 tem como diretrizes a Portaria GM/MS nº 3.632, de 21 de dezembro de 2020, tendo como objetivo consolidar e sistematizar os trabalhos realizados, na última década, pelo Ministério da Saúde, para fins de informatização do sistema de saúde no Brasil. Disponível em: <https://www.gov.br/saude/pt-br/assuntos/saude-digital/a-estrategia-brasileira/a-estrategia->

sistematização e consolidação da saúde digital nacional, com os anos de 2020 a 2028 como marco de sua aplicação.

Importante perceber que a visão estratégica de saúde digital para o Brasil apresenta perspectivas para estabelecimento da plataforma digital que integre o sistema de saúde brasileiro, até o ano de 2028, especialmente a partir de avanços nas experiências de projetos do programa Conecte SUS, promovendo a sistematização de ações dentro do Sistema Único de Saúde – SUS, como no caso da implantação efetiva da Rede Nacional de Dados em Saúde (RNDS), que foi institucionalizada pela Portaria GM/MS nº 1.434, de 28 de maio de 2020⁴, com ações de integração da saúde complementar e saúde privada, a partir da troca de dados entre pontos identificados como Rede de Atenção à Saúde (RAS), com a expectativa de integração das 27 unidades federativas, agora em 2023⁵.

Nesse contexto, as iniciativas propiciam que a RNDS ofereça serviços essenciais de saúde digital, mas acaba por criar portas para a interseção (interoperabilidade) entre sistemas de informação de saúde de todos os setores dessa área no Brasil.

De tal maneira, apresenta-se a utilização de dados pessoais sensíveis pelo sistema, que, ao serem tratados, passam a informar a rede de saúde nacional, sendo criada informações sobre os usuários da saúde, que passam a transitar entre organizações da saúde pública e privada.

Por tal fato, emerge no presente trabalho o questionamento (problema) quanto ao tratamento de dados pessoais sensíveis na política nacional da saúde digital e se há limites no seu uso, considerando a diversidade de atores e dos interesses das organizações presentes no complexo processo da saúde brasileira, apresentando interseções da LGPD diante da fragilidades do sistema e buscando um parâmetro limitador para o uso desses dados.

brasileira. Acesso em: 20 mar. de 2023.

⁴ A PORTARIA Nº 1.434, DE 28 DE MAIO DE 2020 institui o Programa Conecte SUS e altera a Portaria de Consolidação nº 1/GM/MS, de 28 de setembro de 2017, para instituir a Rede Nacional de Dados em Saúde e dispor sobre a adoção de padrões de interoperabilidade em saúde. Disponível em <https://www.in.gov.br/en/web/dou/-/portaria-n-1.434-de-28-de-maio-de-2020-259143327>.

Acesso em: 2 abr. de 2023.

⁵ Os demais eixos se apresentam como: eixo 2 – construção do arcabouço organizacional, legal, governança e regulatório da saúde digital; eixo 3 – implementação do ambiente conceitual, normativo, educacional e tecnológico. Referidos eixos irão ser tratados de forma indireta pelo presente trabalho.

O trabalho se desenvolverá através do objetivo geral que visa analisar o tratamento de dados pessoais sensíveis na política nacional da saúde digital e quais os limites do seu uso, à luz da Lei Geral de Proteção de Dados, complementando o desenvolvimento da pesquisa por meio da compreensão das diretrizes da Visão da Estratégia de Saúde Digital para o Brasil (ESD28), quanto à integração da saúde pública e privada, a partir do tratamento de dados dos usuários.

De tal maneira, considerando a temática a ser pesquisada, os sujeitos envolvidos e os objetivos, a pesquisa apresenta o método procedimental dogmático, considerando a investigação proposta a partir do trinômio doutrina, legislação e jurisprudência, cuja união de tais elementos remete à validade da conjuntura jurídica contemporânea do Estado Democrático e Social.

A análise consubstanciará a aproximação dos fundamentos doutrinários à realidade fática, via interpretação sistemática, através da pesquisa exploratória, utilizando-se uma pesquisa qualitativa, quanto a sua natureza, e, quanto aos objetivos, de caráter descritiva, com levantamento bibliográfico e documental utilizando-se de livros, periódicos, legislações, em especial a Constituição Federal e a Lei nº 13.079, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados), com a redação dada pela Lei nº 13.853/2019, bem como o Plano de Estratégia de Saúde Digital (ESD28), demais legislações afins e diferentes trabalhos de acadêmicos que se relacionam com o objeto de estudo (GIL, 2008, p. 16).

A pesquisa possibilitará resultados parciais sobre a possível identificação de limites no uso de dados pessoais sensíveis na política nacional da saúde digital, considerando a visão da Estratégia de Saúde Digital (ESD28) e o uso da principiologia da LGPD na transmissão de dados a ser realizada na interconexão entre sistema público e privado de saúde.

2 PANORAMA JURÍDICO DO DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS E A SAÚDE DIGITAL

O ser humano é uma animal que necessita viver em sociedade, ou seja, junto a outras pessoas, até mesmo para a sua sobrevivência e desenvolvimento, o que não significa abrir mão de um espaço mais restrito, de intimidade e privacidade,

igualmente necessário para desenvolver uma vida com qualidade. É inimaginável a existência de uma vida *boa* estando total e permanentemente exposto aos olhos dos outros indivíduos.

Assim, embora a noção de privacidade (*privacy*) exista desde tempos longínquos, não se podendo especificar uma data de quando ocorreu o seu surgimento, uma formatação mais estruturada no âmbito do direito adveio com o trabalho formulado pelos norte-americanos Louis Dembitz Brandeis e Samuel Dennis Warren, em que se estabeleceu como sendo um direito individual de *não intromissão*, que ia além do corpo do indivíduo (WARREN; BRANDEIS, 1890, p. 213), muito embora o direito à privacidade não existisse na Constituição dos Estados Unidos da América. Até mesmo atualmente o entendimento formulado por Brandeis e Warren continua a exercer grande influência,⁶ muito embora não seja possível reconhecer que essa teoria continue sendo aplicável a todos os *atos da vida*, visto que não consegue solucionar, de forma adequada, situações derivadas das inovações tecnológicas, em especial quando relacionadas com o mundo digital.

A privacidade,⁷ que se caracteriza como um direito especial de personalidade, está estabelecida como um direito fundamental na Carta Política de 1988 (art. 5º, X), é de difícil definição (SARLET; MARINON, MITIDIERO, 2021, p. 451). Apesar disso, pode ser caracterizado, utilizando a lição de Ingo W. Sarlet, como um direito de controle sobre uma parte da vida privada, em que é possível o desenvolvimento de “sua individualidade”, o que compreende um espaço reservado para se recolher e refletir, bem como o controle “sobre as informações a respeito de sua vida pessoal” (SARLET; MARINON, MITIDIERO, 2021, p. 460).

Saliente-se que o direito fundamental à proteção de dados pessoais somente foi expressamente introduzido no sistema jurídico brasileiro pela Emenda Constitucional nº 115/2022, que acrescentou o inciso LXXIX no art. 5º da

⁶ Com o passar do tempo, ocorreu uma significativa transformação/ampliação do conceito de privacidade, para além do denominado *right to be et alone*, abrangendo situações como o direito do indivíduo estabelecer e criar sua própria identidade, de forma isolada e nas relações sociais (ESPINOSA, 2012, p. 969).

⁷ Ressalta-se que o presente estudo é limitado à privacidade do indivíduo, e não à sua intimidade, que, ao menos para uma parcela da doutrina, nada mais é do que uma esfera mais restrita, possuindo uma proteção mais ampla. Por isso, as considerações feitas a respeito da privacidade igualmente são válidas para a intimidade.

Constituição Federal de 1988. Entretanto, é de se referir que a doutrina, mesmo antes da expressa constitucionalização da proteção de dados pessoais com um direito fundamental, já o assim entendia, até porque ele surge a partir da extração de parcelas de outros direitos fundamentais, inclusive o da privacidade.

Veja-se que Ingo W. Sarlet, mesmo antes da Emenda Constitucional nº 115/2022, afirmava que “o direito à proteção de dados pessoais pode ser associado ao direito à privacidade (no sentido de uma ‘intimidade informática’) e ao direito ao livre desenvolvimento da personalidade, que inclui o direito à livre disposição dos dados pessoais” (SARLET; MARINON, MITIDIERO, 2021, p. 487), com o que se pode asseverar que o direito hoje existente no art. 5º, LXXIX, da CRFB/88, é, em parte, uma particularidade (juntamente com parcelas extraídas de outros direitos fundamentais) do direito à privacidade. Por esse motivo, é possível afirmar que a utilização de dados pessoais atinge, em um grau maior ou menor, dependendo das circunstâncias do caso concreto, a privacidade do indivíduo.⁸

Nesse sentido, deve-se considerar que o mundo e a sociedade atual estão muito diferentes daqueles que existiam quando do surgimento da Constituição brasileira de 1988. Atualmente, nos encontramos numa sociedade informacional, em que a geração, o conhecimento e a transmissão da informação tornam-se fontes fundamentais de produtividade e poder e em que a informação penetra em toda a estrutura social (CASTELLS, 1999, p. 87).

Consoante afirma Klaus Schwab (2016, p. 23), a sociedade encontra-se em uma quarta revolução industrial, que se caracteriza por uma inter-relação entre a tecnologia e os mundos digital, físico e biológico, com o que parece correta a afirmação de Bruno Latour, no sentido de que somos animais sociotécnicos.⁹

⁸ Moisés Barrio Andrés sustenta que “no contexto da Internet, é geralmente aceito que a privacidade é o direito de determinar quando, como e em que medida os dados pessoais podem ser compartilhados com terceiros” [tradução livre] (2020, p. 194).

⁹ “Conceber humanidade e tecnologia como polos opostos é, com efeito, descartar a humanidade: somos animais sociotécnicos e toda interação humana é sociotécnica. Jamais estamos limitados a vínculos sociais. Jamais nos defrontamos unicamente com os objetivos. [...] A ilusão da modernidade foi acreditar que, quanto mais crescemos, mais se extremam a objetividade e a subjetividade, criando assim um futuro radicalmente diferente de nosso passado. Após a mudança de paradigma em nossa concepção de ciência e tecnologia, sabemos agora que isso nunca acontecerá e, na verdade, *nunca* aconteceu. [...] [Os artefatos] merecem ser alojados em nossa cultura intelectual como atores sociais de pleno direito. Os artefatos somos nós. O alvo de nossa filosofia, teoria social e moralidade cifra-se em inventar instituições políticas capazes de absorver essa grande história, esse vasto movimento espiral, esse labirinto, esse fato.” (LATOUR, 2001, p. 245).

Some-se a tudo isso o fato da sociedade atual estar hiperconectada, existindo uma vasta quantidade informações fluindo diariamente, principalmente entre computadores e dispositivos móveis de comunicação, sendo que é nessa hiperconexão diária entre dispositivos que se dá a transferência de dados pessoais, em muitos casos desconhecida por parte do indivíduo ou, caso conhecida, de pouco significado para ele, por não acreditar que isso possa lhe causar algum dano ou, ainda, por possuir uma visão diversa de privacidade da que existia no final dos anos 2000.

Assim, vê-se que atualmente há, ao lado de uma sociedade física/material (que podemos chamar de analógica), uma sociedade que se caracteriza como sendo digital, em que uma vasta gama de informações, das mais variadas espécies, circula a cada segundo.¹⁰

Nesse contexto, ocorre a coleta de dados de saúde dos usuários do sistema de saúde digital (*eHealth*),¹¹ obtidos (principalmente) a partir da inclusão em plataformas, que estão em rede, das informações oriundas de exames clínicos, laboratoriais, de imagem, de prontuários eletrônicos do paciente (PEP), extraídas de dispositivos móveis de medicina, de saúde ou fitness e a inserida pelo médico ou outro profissional de saúde em sistema informatizado em que está a ficha do paciente, o que proporciona sua futura análise, tratamento, transmissão e uso, inclusive para fins diversos dos que previstos inicialmente.

¹⁰ Em janeiro de 2022, a *Datareportal* apontou a existência de 4,95 bilhões de usuário da *internet* (KEMP, 2022). Já no Brasil, de acordo com a Pesquisa Nacional por Amostra de Domicílios (PNAD) de 2021, 90 % dos domicílios no país tinham acesso à *internet* (NERY; BRITO, 2022).

¹¹ A Organização Mundial de Saúde define a *eHealth* como sendo "o uso de tecnologias de informação e comunicação (TIC) para a saúde." (WORLD HEALTH ORGANIZATION). Por sua vez, o Comitê Gestor da Estratégia e-Saúde do Ministério da Saúde brasileiro afirma que: "de forma mais ampla 'e-Saúde' representa o contexto da prática de atenção à saúde facilitada e aperfeiçoada pelo uso de tecnologias modernas de Informação e Comunicação (TIC), considerando as aplicações dessas tecnologias na organização, gestão e agilidade dos processos de atendimento ao paciente, no compartilhamento de informações, na garantia de maior qualidade e segurança das decisões clínicas, no acompanhamento de pacientes, em políticas de Saúde pública, na compreensão dos fatores determinantes do bem estar do cidadão, na detecção e controle de epidemias, entre tantas outras possibilidades." (BRASIL, Ministério da Saúde, Estratégia de e-Saúde para o Brasil, 2017, p. 17). É de se ressaltar que em 2019 o referido Comitê foi substituído pelo Comitê Gestor da Estratégia da Saúde Digital (Resolução nº 46 do Ministro da Saúde, de 29 de agosto de 2019), sendo que a partir de então, aparentemente, saúde digital passou a ser a denominação oficialmente utilizada pelo Ministério da Saúde como o correspondente em língua portuguesa ao *eHealth*.

Veja-se que a crescente evolução dos programas (constituídos por algoritmos),¹² que são uma sequência de ordens a serem obedecidas, visando dar solução a um problema específico ou realizar uma tarefa¹³, de avaliação de dados pessoais, em conjunto com a hiperconectividade dos dias atuais, faz com que os dados médicos anonimizados sejam suscetíveis de desanonimização ou, ainda, possam ser utilizados para a construção de categorias, trazendo o potencial risco de estigmatização, de discrimen ou de exclusão dos indivíduos que o compõem (SARLET, G.; MOLINARO, 2019, p. 202-203).

Por tudo isso, é fundamental que o indivíduo possa ter o controle dos seus dados (digitais) pessoais de saúde, isto é, que ele possa exercer de forma efetiva a autodeterminação informativa,¹⁴ principalmente se considerarmos as características de tais informações e os danos que o seu irregular uso podem causar para o indivíduo.

A respeito da autodeterminação informativa, em face da sua estrutura normativa, caracteriza-se com um princípio, não estando acima dos demais direitos, como o da privacidade ou o da personalidade, possuindo uma dupla dimensão, individual e coletiva, em que na primeira é garantida a cada um decidir sobre acessar, utilizar e difundir os seus próprios dados pessoais, bem como, no tocante à segunda, se "constitui precondição para uma ordem comunicacional livre e democrática, distanciando-se, nessa medida, de uma concepção de privacidade individualista e mesmo isolacionista à feição de um direito de estar só (*right to be alone*)" (SARLET,

¹² Para a definição tradicional de algoritmo, ele dever ser considerado como sendo "uma lista de instruções que levam o usuário diretamente a uma resposta ao resultado específico, dadas as informações disponíveis". (MODELI; SANTOS; JULIASZ; DAUN; PAIÃO, 2020, p. 78).

¹³ Considerando que um algoritmo é composto de *ordens* (linhas de comando) formuladas por uma pessoa humana, tais *ordens* sempre trazem subjacente a noção de mundo que essa pessoa possui, em face do que correta é a assertiva de Wittgenstein, para quem "os limites de minha linguagem significam os limites de seu mundo" (2001, p. 245, proposição 5.6). Diante disso, é de suma importância o que se denomina de *privacy by design*, que é a "metodologia que visa proteger a privacidade do usuário desde a concepção de quaisquer sistemas de tecnologia da informação ou de práticas de negócio que sejam concernentes ao ser humano" e de "*privacy by default*, que se refere à metodologia que adota por padrão a configuração de privacidade mais restritiva possível na fase da coleta de dados pessoais por qualquer sistema de tecnologia da informação, a fim de garantir a proteção dos dados pessoais de forma automática, ainda que nenhuma interação com a máquina tenha sido feita pelo usuário nesse sentido." (JIMENE, 2019, p. 336).

¹⁴ A autodeterminação informativa pode ser definida como "o direito que tem o indivíduo de escolher com quem pretende compartilhar suas informações, partindo do pressuposto de que pode vetar qualquer ingerência não consentida eporquanto são dados e informações de caráter pessoal que quer manter em sigilo." (RUARO, 2015, p. 45).

2021, p. 32).

É preciso salientar que com a crítica em relação à desnecessidade de consentimento do titular dos dados de saúde, ou do seu responsável, em uma grande variedade de situações, não se está defendendo a necessidade de autorização para o acesso à totalidade desses dados pessoais, sob pena de realizarmos uma limitação excessiva, afetando até mesmo o núcleo essencial da disposição constitucional que estabelece a tarefa estatal de incentivo e promoção ao desenvolvimento científico e à pesquisa, além do direito fundamental à saúde – art. 6º, *caput*, e art. 196, da CRFB/88 (MARQUES, 2018, p. 2082).

Porém, entende-se necessário realizar um aperfeiçoamento da legislação infraconstitucional, visando uma proteção mais em conformidade com os direitos fundamentais, em especial daqueles que utilizam o sistema de saúde nacional, pois seus dados serão transmitidos para uma base que terá uma comunicação (uma integração) entre a rede pública e a rede privada.

3 ASPECTOS GERAIS DA ESTRATÉGIA DE SAÚDE DIGITAL NO BRASIL

No Brasil, a Estratégia de Saúde Digital é apresentada pelo Ministério da Saúde por meio de um panorama visionário de oito anos, iniciando em 2020 e findando em 2028, com a sistematização e implantação de um rol de normativas construídas nos últimos dez anos no país, consolidando a perspectiva da saúde digital como um sistema plenamente integrado às 27 unidades federativas (BRASIL, Estratégia de Saúde Digital, 2020, p. 11).

De tal maneira, a Estratégia de Saúde Digital (a partir de agora identificada no texto como ESD28) é fruto da consolidação de vários documentos oficiais, que interagem com políticas públicas no campo da saúde, presentes no Plano Nacional de Saúde (BRASIL, PNS, 2016, p. 20)¹⁵, com ênfase na Política Nacional de Informação e Informática em Saúde – PNIIS (BRASIL, PNIIS, 2016, p. 15), que estabeleceu o conceito de saúde digital no Brasil.

¹⁵ Por ter vigência de 4 em 4 anos, atualmente, o Plano Nacional de Saúde encontra-se na versão 2020-2023, com revisão ocorrida no ano de 2021, conforme informação do Ministério da Saúde.

Nesse contexto, a ESD28 possui itens já executados, anos de 2015 a 2019, que apresentaram a implementação de eixos, inicialmente com a internalização das diretrizes e metodologias da Organização Mundial de Saúde, passando pela condução da elaboração da visão estratégica e do plano de ação, além do monitoramento e avaliação da saúde digital.

Da mesma forma, a ESD28 possui itens em execução, que revisam os documentos da última década e impulsionam a continuidade de ações para reafirmação das diretrizes da saúde digital no Brasil¹⁶. Nesse fluxo atual, há três eixos, baseados nas perspectivas das ações propostas em um outro documento presente nesse ambiente de informatização da saúde brasileira, que é o Plano de Ação, Monitoramento e Avaliação (PAM&A – 2019-2023)¹⁷.

O PAM&A identificou, priorizou e integrou, coordenadamente, programas e projetos da saúde em meio à busca por sua informatização, implantando iniciativas para materializar a estratégia de saúde, como, por exemplo, na composição do Conecte SUS, que fomentou a informatização e a troca de informações entre os sistemas da Rede de Atenção à Saúde, configurando o marco para o alinhamento da ESD28 à nova política nacional de informação e informática em saúde (PNIIS, 2021), com base na Portaria GM/MS nº 1.768, de 30 de julho de 2021.

Percebe-se, então, que a visão estratégica de saúde digital no Brasil estabelece um gradativo fortalecimento da Rede Nacional de Dados de Saúde (RNDS), tendo como objetivo ser estabelecida e reconhecida, até 2028, como a plataforma digital para os serviços de saúde do Brasil, oportunizando inovação e informação aos beneficiários do sistema de saúde, passando por pacientes, comunidades, e atingindo profissionais da saúde e gestores da saúde no país.

Nesse ponto, ressalta-se que a Visão Estratégica de Saúde Digital é a primeira parte da ESD28, que tem como objetivo reafirmar, atualizar e expandir os conteúdos da Estratégia de e-Saúde, consolidando os projetos propostos no PAM&A 2019-2023, até 2028, com ênfase no Programa Conecte SUS, em particular as iniciativas

¹⁶ O Ministério da Saúde apresentou, através do Departamento de Informática do SUS, a Estratégia de Saúde Digital para o Brasil 2020-2028.

¹⁷ O Ministério da Saúde apresentou o Plano de Ação, Monitoramento & Avaliação da Estratégia de Saúde Digital para o Brasil 2019-2023 (BRASIL, Ministério da Saúde, Plano de Ação, Monitoramento & Avaliação da Estratégia de Saúde Digital para o Brasil 2019-2023, 2020).

Rede Nacional de Dados em Saúde (RNDS) e o Informatiza APS.

A Rede Nacional de Dados de Saúde (RNDS) é institucionalizada pela Portaria GM/MS nº 1.434, de 28 de maio de 2020, e nela se estabelece o importante conceito de plataforma digital padronizada da saúde no Brasil, que leva a promoção das referidas interações de sistemas da saúde pública e privada, com base na troca de informações entre os ditos pontos da Rede de Atenção à Saúde (RAS).

Segundo o Ministério da Saúde, na consolidação da RNDS, o Sistema Único de Saúde terá a operacionalidade conjunta da Saúde Suplementar e da Saúde Privada, com a consequência direta para os usuários, que, ao utilizarem tais setores, com a transmissão conjunta de seus dados e da informação de saúde utilizadas, pois ambos estarão disponíveis em quaisquer dos setores, considerando que os usuários podem transitar entre organizações de saúde públicas e privadas (BRASIL, ESD28, 2020, p. 11).

Assim, a visão estratégica de saúde digital se personifica na possibilidade da efetivação da saúde digital, através da relação direta entre políticas públicas e políticas de saúde, considerando diretrizes de governança digital, consolidando a Política Nacional de Saúde, concretizando a RNDS, que tem como objetivo precípua a promoção de troca de informações entre pontos da Rede de Atenção à Saúde, fato que permitirá que os setores públicos e privados possam ter a transição de dados e a continuidade na relação de cuidado, própria da saúde (BRASIL, ESD28, 2020, p. 20).

4 INTERSEÇÕES DA LGPD NA SAÚDE DIGITAL: fragilidades no tratamento de dados no e-Saúde

Diante do debate pontuado, percebe-se que a troca de informações entre os pontos da Rede de Atenção à Saúde (RAS) fomentará a RNDS como plataforma nacional de inovação, informação e serviços digitais em saúde, sendo compostas por várias linhas de possíveis agentes que irão interagir com os dados coletados.

O Ministério da Saúde (MS), através de estudos da Estratégia da Saúde Digital,¹⁸ elenca que no horizonte de 2020 a 2028 o Brasil terá uma integração entre

¹⁸ Os estudos são retratados por documentos oficiais do Ministério da Saúde.

atores que cuidarão da gestão da unidade de saúde, da gestão de operadoras, dos serviços de informação e alerta, além de possibilitar o tráfego de dados em laboratórios, centros de pesquisa e desenvolvimento, atendimento de urgência e emergência, farmácias, gestores, a partir de informações de comunidades de usuários, possibilitando a verificação, em última análise, da saúde populacional.

Nesse contexto, retoma-se a problemática da pesquisa, que envolve o questionamento sobre o tratamento de dados pessoais sensíveis na política nacional da saúde digital e quais os limites no seu uso, considerando a diversidade de atores e uma possível utilização de dados do sistema público, no sistema privado.

De tal maneira, para a total integração, o sistema utilizará programas, que estarão alimentados com os dados dos usuários, e, assim, de maneira apenas a se conjecturar, poderá se ter um uso enviesado de tais dados, para além da medicina preventiva, do uso benéfico de dados.

Ora, muito embora nenhuma tecnologia, que sempre é uma obra do ser humano, possa ser considerada como neutra (NEVES; CARVALHO, 2018, p. 9), já que leva o traço do seu criador, é preciso reconhecer que a ausência dessa neutralidade decorre mais do seu uso indevido, pernicioso à pessoa humana ou ao ambiente em que ela vive, para obter uma vantagem econômica ou adquirir poder. Assim, o desenvolvimento tecnológico igualmente afeta, em graus diversos, a pessoa humana, em razão do que é necessária sua regulação pelo direito.

Esse talvez seja o contexto da sociedade de informação, onde a rapidez com que ocorre o desenvolvimento da tecnologia relacionada com as avaliações de dados pessoais (em especial do *big data*¹⁹ e a *inteligência artificial*²⁰ e suas vertentes –

¹⁹ As definições de *big data* evoluíram bastante desde o surgimento dessa tecnologia, a ponto de hoje não haver apenas um sentido. (CANITO, 2017, p. 15-18). "O termo *Big Data* refere-se a situações em que as tecnologias digitais são utilizadas para lidar com grandes e diversas quantidades de dados e às várias possibilidades de combinação, avaliação, e processamento desses dados por autoridades privadas e públicas em diferentes contextos", caracterizando-se pelos cinco "Vs": volume, variedade, velocidade, veracidade e valor (HOFFMANN-RIEM, 2021, p. 16-17).

²⁰ Inteligência artificial pode ser definida como "a atividade devotada a tornar as máquinas inteligentes e inteligência é a qualidade que permite um ente funcionar apropriadamente e com predição sobre o seu ambiente [tradução livre]" (NILSSON, 2010, p. 13).

machine learning,²¹ *deep learning*²² e *processamento de linguagem natural*²³), tornou a LGPD (Lei nº 13.709/2018) já ultrapassada no tocante a algumas tecnologias, como as que são utilizadas na saúde digital, mas que possui um arcabouço principiológico passível de utilização como limitador mínimo para o tratamento de tais dados.

Por esse motivo, e tendo em vista o atual momento de consolidação e ampliação da sociedade em rede (que igualmente está inserida em um novo formato de sociedade, a sociedade digital), em que a coleta, tratamento, análise, transmissão e uso dos dados pessoais ocorre de forma cada vez mais veloz, eficiente e sem que o indivíduo tenha a exata dimensão da forma como se dá o uso de suas informações, mesmo que estejam anonimizadas, tal situação pode lhe acarretar consequências gravosas.

Nesse ponto, pode-se exemplificar a irregular utilização de dados pessoais na área da saúde, objeto de julgamento proferido pelo Tribunal de Justiça de São Paulo, que condenou um laboratório pela utilização indevida/não autorizada de informações de uma mulher que tinha feito exame de gravidez, sendo que pouco tempo depois veio a ocorrer um aborto espontâneo.

No caso, após alguns dias, por meio do aplicativo WhatsApp, a paciente recebeu mensagens de um laboratório de criobiologia oferecendo seus serviços de coleta e armazenamento de cordão umbilical, sem, contudo, ter um único contato com a empresa. No julgamento, o Tribunal condenou o laboratório ao pagamento de indenização por danos morais a favor da autora, porquanto fez uso de dados pessoais sensíveis sem autorização, em face do que a "conduta da ré, seguramente, além de representar violação ao direito de privacidade, fez a autora reviver sofrimento

²¹ O aprendizado de máquina (em inglês, *machine learning*) "é o processo de indução de uma hipótese a partir de uma experiência. A capacidade de melhorar, de aprender, de otimizar o desempenho de uma tarefa é fundamental para noção de inteligência." (CALIENDO, 2020, p. 496).

²² "O *deep learning* se refere à hipótese na qual a IA aprende de maneira assemelhada às redes neurais humanas, sendo outra modalidade avançada de *machine learning*. A IA, nesse patamar, aprende representações de dados com múltiplos níveis de abstração. (FREITAS; FREITAS, 2020, p. 32).

²³ "O *Processamento de Linguagem Natural (natural language processing – NLP)* é o ramo da IA que trata da interface entre a linguagem natural (humana) e a linguagem de computador. Durante décadas, tem sido um grande objetivo o esforço de máquina para uma maciça tradução em tempo real, de um idioma para outro. O mesmo esforço tem sido despendido para alcançar melhores resultados em processamento de imagens (*image processing*) e processamento de voz (*speech processing*)." (CALIENDO, 2020, p. 496).

decorrente da perda gestacional".²⁴

Outro exemplo, que bem demonstra a fragilidade do sistema de saúde, quanto aos dados pessoais nele contido, é o caso noticiado pela imprensa jurídica nacional, que relatou o caso de um enfermeiro que, em uma ação trabalhista em trâmite na 81ª Vara do Trabalho de São Paulo/SP, para fins de comprovação de seu direito (decorrente de diversas falhas e do descumprimento de obrigações por parte da empresa), juntou planilhas do Sistema de Gerenciamento de Internações.

Em vista do ocorrido, a Juíza da causa reconheceu que o autor violou a intimidade e privacidade de terceiros, clientes da demandada, além de violar a LGPD, pois utilizou de forma ilícita os dados pessoais sensíveis. Diante disso, o pleito de demissão indireta do trabalhador foi julgado improcedente, sendo ele punido por falta praticada com a dispensa por justa causa (CONSULTOR JURÍDICO, 2023).

Ainda, em pesquisa publicada em 2021 no BMJ (*British Medical Journal*), uma equipe de pesquisadores da Universidade Macquarie, em Sydney (Austrália), a partir de uma análise de mais de 20.000 aplicativos *Android* de *mHealth* (que vão desde contadores de calorias até verificadores de sintomas e aplicativos médicos), nos quais foram analisados o código de cada um desses aplicativos para funções e permissões de coleta dos dados dos usuários, chegaram a preocupantes resultados, que podem ser assim resumidos:

- 1) os aplicativos de saúde e fitness eram mais propensos a incluir a capacidade de coletar e compartilhar dados do usuário do que os aplicativos médicos; uma significativa porcentagem dos aplicativos de saúde foi codificada com a capacidade de coletar dados que poderiam ser usados para construir perfis *on-line* de usuários. Por exemplo, mais de 60% dos aplicativos de saúde tinham a

²⁴ O acórdão foi assim ementado: "Responsabilidade civil. Indenização por danos morais. Ação cominatória. Tratamento de dado sensível pela Lei nº 13.709/2018. Autora, que, após perda gestacional, recebeu oferta da ré a respeito de serviços de coleta e armazenamento de cordão umbilical. Ré que confirma ter recebido informações a respeito da autora de terceiros. Dados sensíveis, a respeito da gravidez da autora, que não poderiam ter sido objeto de compartilhamento, nos termos do art. 11, § 4º, da Lei nº 13.709/18. Ré que fez uso indevido de dado sensível pertencente à autora com finalidade lucrativa. Prospecção de novos clientes. Ato ilícito caracterizado. Violação do direito de privacidade da autora. Indenização corretamente determinada na sentença (R\$ 10.000,00). Ré que tem a obrigação legal de identificar o responsável pela coleta do dado da autora, o que se deu sem consentimento. Sentença de procedência dos pedidos mantida. Recurso desprovido." (BRASIL, São Paulo, 2022).

capacidade de coletar identificadores MAC e cookies, que podem ser usados para identificar usuários em diferentes aplicativos e sites. Cerca de um terço coletou endereços de e-mail dos usuários, e um quarto poderia coletar a localização da torre de celular;

2) a maioria desses códigos para coleta de dados estava relacionada a serviços de terceiros, como *Google Analytics*, *Google Ads*, *Github* ou *Facebook*, sendo que os serviços do Google sozinhos representaram mais de um terço das operações de coleta de dados no código dos aplicativos;

3) em torno de 88% dos aplicativos foram construídos com a capacidade de coletar ou compartilhar dados de usuários com terceiros (incluindo serviços de publicidade e rastreamento);

4) uma porcentagem significativa dessas transmissões de dados, cerca de 23%, não utilizava protocolos de comunicação seguros. Por exemplo, informações não criptografadas sobre a senha do usuário e localização (*gps* – global positioning system);

5) menos da metade dos aplicativos compartilhavam dados de usuários de uma maneira consistente com sua política de privacidade, e cerca de 28% dos aplicativos não forneceram uma política de privacidade;

6) "a coleta de informações pessoais do usuário é uma prática generalizada em aplicativos *mHealth*, e nem sempre transparente e segura [tradução livre]" (TANGARI, IKRAM; IJAZ; KAAFAR; BERKOVSKY, 2021).

De outro lado, é preocupante o fato de a Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018, art. 11, II) estabelecer que os dados sensíveis de saúde²⁵ não necessitam do consentimento de seu titular ou responsável para fins de estudos a serem realizados por órgãos de pesquisa ou mesmo para a tutela da saúde, quando realizados de forma exclusiva por profissionais, serviços da área da saúde ou por autoridade sanitária, sendo também permitida a comunicação e o uso compartilhado das informações entre controladores de dados sensíveis referentes à saúde nas hipóteses relacionadas com a prestação de serviços nessa área, de assistência farmacêutica e de assistência à saúde (exceto para as operadoras de planos

²⁵ Os dados de saúde, para CRISTEA UIVARU, "(...) consistem nas informações que se referem à saúde passada, presente ou futura, em pessoais saudáveis ou doentes, com enfermidades de caráter físico ou psicológico, e que inclui a dependência ao álcool ou às drogas [tradução livre]" (2018, p. 46),

privados de assistência à saúde quando visem à prática de seleção de riscos na contratação de qualquer modalidade ou a contratação ou exclusão de beneficiários), incluídos os serviços auxiliares de diagnose e terapia, desde que em benefício dos interesses dos titulares de dados.

Ademais, é possível o compartilhamento dos dados pessoais de saúde para permitir a portabilidade dos dados pelo titular ou, ainda, para realizar transações financeiras e administrativas resultantes do uso e da prestação dos serviços, o cumprimento de obrigação legal ou regulatória pelo controlador e o tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos.

Logo, há uma grande variedade de situações em que os dados pessoais relacionados com a saúde encontram-se disponíveis para compartilhamento entre os operadores, pessoas jurídicas de direito privado ou público, sem que para tanto seja necessário o consentimento do titular ou do responsável (e também sem que o titular dos dados saiba sobre tais compartilhamentos), diante do que temos uma excessiva invasão no âmbito da privacidade desses indivíduos, da dignidade da pessoa humana (em especial no que toca com o livre desenvolvimento da personalidade) e, também, no tocante ao direito fundamental à proteção de dados pessoais (no que se inclui a autodeterminação informativa).

CONCLUSÕES

A compreensão e sistematização de dados na saúde digital nacional, com base nas metas impostas pelo governo, em seu plano nacional, diante do horizonte 2020 a 2028, com base no marco de aplicação do uso de dados sensíveis no primeiro eixo da Estratégia de Saúde Digital (ESD28), tem como meta inicial o fortalecimento, consolidação e ampliação de ações propostas anteriormente no Plano de Ação, Monitoramento e Avaliação de Saúde Digital para o Brasil (PAM&A 2019-2023), fato que inclui ações previstas no Programa Conecte SUS, especialmente a iniciativa da Rede Nacional de Dados em Saúde (RNDS), que tornará efetiva a interconexão entre sistema público e privado de saúde no Brasil.

No entanto, o contexto abordado apresenta uma perspectiva, no atual momento, de se ter uma insuficiência protetiva dos dados pessoais sensíveis dentro da Estratégia de Saúde Digital (ESD28), pois os atores que participarão da rede nacional de dados da saúde possuem interesses diferenciados, visto que se encontram, em parte, dentro da sistemática do mercado, o que envolve planos de saúde, seguros de saúde, indústria farmacêutica etc.

Nesse sentido, é possível retomar a problemática da pesquisa quanto ao tratamento de dados pessoais sensíveis na política nacional da saúde digital, pois é necessário um limite no seu uso, quer seja no consentimento informado, quer seja na construção de grande fluxo de informação para que a comunidade, principalmente aqueles integrantes mais carentes, possam saber o porquê da disponibilidade de seus dados e quais benefícios estarão a receber, excluindo qualquer tipo de construção de algoritmos que possam levar a discriminações ou exclusões sistêmicas.

Essa perspectiva considera a diversidade de atores e dos interesses das organizações presentes no complexo processo da saúde brasileira, apresentando interseções da LGPD diante das fragilidades do sistema e buscando um parâmetro limitador para o uso desses dados.

Por tal fato, o percurso do horizonte da ESD28 deve ser trilhado por aprimoramentos do tratamento e uso dos dados sensíveis, a fim de efetivar, de forma real e robusta, as disposições protetivas da LGPD, no contexto de interconexão entre sistema público e privado de saúde.

De tal maneira, a utilização de dados pessoais sensíveis pela sistemática da Saúde Digital, no Brasil, remete à construção de uma gama de informações que podem apresentar externalidades negativas aos usuários do sistema.

Nesse contexto, como conclusões parciais, aponta-se que a rede de saúde nacional, ao ser alimentada por uma gama de dados, peculiares a cada usuário, poderá ocasionar uma construção de perfis adequados, ou não, que modificam, ou não, a teia construída através dos dados, o que é refletido na indústria de medicamentos, na precificação de planos de saúde, na política de saúde do trabalho etc., fatos que obrigam a presença do crivo das disposições da LGPD, para que haja o respeito de garantias protetivas mínimas de direitos sensíveis à vida de cada

usuário da rede nacional de saúde e o uso adequado aos verdadeiros fins da rede digital, que é a melhoria e modernização da prestação essencial do serviço universal da saúde.

REFERÊNCIAS

BARRIO ANDRÉS, Moisés. *Fundamentos del derecho de internet*. 2ª ed. Madrid: Centros de Estudios Políticos y Constitucionales, 2020.

BRASIL. *Constituição da República Federativa do Brasil*. Brasília, DF: Senado Federal, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 29 out. de 2022.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD)*. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 20 jan. de 2023.

BRASIL. Ministério da Saúde. Secretaria-Executiva. Departamento de Monitoramento e Avaliação do SUS. *Plano Nacional de Saúde / Ministério da Saúde, Secretaria-Executiva, Departamento de Monitoramento e Avaliação do SUS*. Brasília: Ministério da Saúde, 2016. Disponível em chrome-extension://efaidnbmnnnibpcajpcgclefindmkaj/https://conselho.saude.gov.br/ultimas_noticias/2016/docs/PlanoNacionalSaude_2016_2019.pdf. Acesso em: 22 fev. de 2023.

BRASIL. Ministério da Saúde. Secretaria-Executiva. Departamento de Monitoramento e Avaliação do SUS. *Política Nacional de Informação e Informática em Saúde / Ministério da Saúde, Secretaria-Executiva, Departamento de Monitoramento e Avaliação do SUS*. Brasília: Ministério da Saúde, 2016. Disponível em: <chrome-extension://efaidnbmnnnibpcajpcgclefindmkaj/https://www.gov.br/saude/pt-br/assuntos/saude-digital/a-estrategia-brasileira/PoliticaNacionaldeInformaoeInformtica.pdf>. Acesso em: 22 fev. de 2023.

BRASIL. Ministério da Saúde. *Política reduzirá riscos relativos à segurança da informação, 20-02-2017*. Disponível em: <https://www.gov.br/saude/pt-br/assuntos/noticias/2017/fevereiro/politica-reduzira-riscos-relativos-a-seguranca-da-informacao>. Acesso em: 22 abr. 2023.

BRASIL. Ministério da Saúde. *Estratégia e-Saúde para o Brasil, 2017. Visão de e-Saúde para o Brasil*. Disponível em: <https://www.gov.br/saude/pt-br/assuntos/saude-digital/material-de-apoio/DocumentodaVisobrasileiraparaaEstratgiaeSade2017.pdf>. Acesso em: 16

out. de 2022.

BRASIL. Ministério da Saúde. Secretaria-Executiva. Departamento de Informática do SUS. *Estratégia de Saúde Digital para o Brasil 2020-2028* / Ministério da Saúde, Secretaria-Executiva, Departamento de Informática do SUS, 2020. Disponível em: https://bvsms.saude.gov.br/bvs/publicacoes/estrategia_saude_digital_Brasil.pdf. Acesso em: 20 mar. de 2023.

BRASIL. Ministério da Saúde. Secretaria-Executiva. Departamento de Informática do SUS. *Plano de Ação, Monitoramento & Avaliação da Estratégia de Saúde Digital para o Brasil 2019-2023*. Brasília: Ministério da Saúde, 2020. Disponível em: <https://www.gov.br/saude/pt-br/assuntos/saude-digital/a-estrategia-brasileira/PlanodeAoMonitoramentoeAvaliao.pdf>. Acesso em: 21 fev. de 2023.

BRASIL. *Portaria nº 1.434, de 28 de maio de 2020*. Institui o Programa Conecte SUS e altera a Portaria de Consolidação nº 1/GM/MS, de 28 de setembro de 2017, para instituir a Rede Nacional de Dados em Saúde e dispor sobre a adoção de padrões de interoperabilidade em saúde. Disponível em <https://www.in.gov.br/en/web/dou/-/portaria-n-1.434-de-28-de-maio-de-2020-259143327>. Acesso em: 2 abr. de 2023.

BRASIL. *Portaria GM/MS nº 1.768, de 30 de julho de 2021*. Altera o Anexo XLII da Portaria de Consolidação GM/MS nº 2, de 28 de setembro de 2017, para dispor sobre a Política Nacional de Informação e Informática em Saúde (PNIIS). Disponível em: <https://www.in.gov.br/web/dou/-/portaria-gm/ms-n-1.768-de-30-de-julho-de-2021-335472332>. Acesso em: 20 abr. de 2023.

BRASIL. *Resolução nº 46 do Ministro da Saúde, de 29 de agosto de 2019*. Institui o Comitê Gestor da Estratégia de Saúde Digital e define a sua composição, as suas competências e as suas unidades operacionais na estrutura do Ministério da Saúde, em substituição ao Comitê Gestor da Estratégia de e-Saúde no Brasil. Disponível em: <https://www.gov.br/saude/pt-br/acao-a-informacao/gestao-do-sus/articulacao-interfederativa/cit/resolucoes/2019/resolu-o-n-46-de-29-de-agosto-de-2019.pdf/@download/file>. Acesso em 16 out. de 2022.

BRASIL. São Paulo. Tribunal de Justiça do Estado de São Paulo. 1ª Câmara de Direito Privado. Responsabilidade civil. Indenização por danos morais. Ação cominatória. Tratamento de dado sensível pela Lei nº 13.709/2018. *Apelação Cível nº 1041607-35.2021.8.26.0100*. Relator Des. Alexandre Marcondes, 17-05-2022. Disponível em <https://www.jusbrasil.com.br/jurisprudencia/tj-sp/1505505819/inteiro-teor-1505505929>. Acesso: em 14 fev. de 2023.

CALIENDO, Paulo. Tributação, inteligência artificial e vieses. In: PISCITELLI, Tathiane; LARA, Daniela Silveira (Coord.). *Tributação da economia digital*. São Paulo: Thomson Reuters Brasil, 2020, p. 491-508.

CANITO, João Miguel Ferreira. *Categorização e Classificação de Notícias de Big*

Data em Tecnologias segundo o Quadrante Mágico de Gartner. Dissertação (Mestrado em Informática e Gestão) – Departamento de Ciências e Tecnologia da Informação, Instituto Universitário de Lisboa. Lisboa, p. 71, 2017. Disponível em: https://repositorio.iscteul.pt/bitstream/10071/15111/1/Disserta%c3%a7%c3%a3o%20-%20Jo%c3%a3o%20Canito_N%c2%ba%2060665_MIGB1.pdf. Acesso em: 8 mar. de 2022.

CASTELLS, Manuel. *A sociedade em rede – A era da informação: economia, sociedade e cultura*. Vol. 1, 3ª ed. São Paulo: Paz e Terra, 1999.

CONSULTOR JURÍDICO. *Empregado viola LGPD em pedido de rescisão indireta e é punido com justa causa*. Disponível em <https://www.conjur.com.br/2023-mar-01/empregado-viola-lgpd-rescisao-indireta-recebe-justa-causa>. Acesso em: 27 mar. de 2023.

CRISTEA UIVARU, Lucia. *La protección de datos de carácter sensible: historia clínica digital y big data em salud*. Barcelona: Bosch, 2018.

ESPINOSA, Manuel José Cepeda (2012). Privacy. In: ROSENFELD, Michel; SAJÓ, Andrés (ed.). *The Oxford Handbook of Comparative Constitutional Law*. Oxford: Oxford University Press, 2012, p. 966-982.

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

GIL, Antonio Carlos. *Métodos e técnicas de pesquisa social*. 6ª ed. São Paulo: Atlas, 2008.

HOFFMANN-RIEM, Wolfgang. *Teoria geral do direito digital: transformação digital: desafios para o direito*. Rio de Janeiro: Forense, 2021.

JIMENE, Camila do Vale. Comentários ao capítulo VII. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coord.). *LGPD: lei geral de proteção de dados comentada*. São Paulo: Thomson Reuters Brasil, 2019, p. 329-354.

KEMP, Simon. Digital 2022: Digital adoption doubled over the past decade. *Datareportal*, 26-01-2022. Disponível em: <https://datareportal.com/reports/digital-2022-digital-adoption-doubled-over-the-past-decade>. Acesso em: 23 mar. de 2023.

LATOURE, Bruno. *A esperança de Pandora: ensaios sobre a realidade dos estudos científicos*. São Paulo: EDUSC, 2001.

MARQUES, Claudia Lima. Comentários ao Capítulo IV, Da Ciência Tecnologia e Informação, e ao art. 218, caput. In: CANOTILHO, Jose Joaquim; MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang.; STRECK, Lênio Luiz (Coords.). *Comentários à Constituição do Brasil*. 2ª ed. São Paulo: Saraiva: Almedina, 2018, p. 2072-2084.

MODELI, Guilherme Marconato; SANTOS, Gustavo Perinetti dos; JULIASZ, Livia Pacheco de Freitas; DAUN, Rafaela Rabelo; PAIÃO, Oliviê Samuel. Eficácia instrumental dos algoritmos jurídicos na tomada de decisão na era da liquidez dos direitos fundamentais. In: NERY, Carmen; BRITTO, Vinícios. Internet já é acessível em 90,0% dos domicílios do país em 2021. *Agência IBGE Notícias*, 16-09-2022. Disponível em: <https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/34954-internet-ja-e-acessivel-em-90-0-dos-domicilios-do-pais-em-2021>. Acesso em: 23 mar. de 2023.

SANTOS, José Eduardo Lourenço dos; LIPPE, Pedro Rodrigues de Freitas; DAUN, Rafaela Rabelo; PAIÃO, Oliviê Samuel (Coords.). *Direitos, novas tecnologias e controle social*. Curitiba: CRV, 2020.

NEVES, Maria do Céu Patrão; CARVALHO, Maria da Graça. O mito da neutralidade axiológica. In: NEVES, Maria do Céu Patrão; CARVALHO, Maria da Graça (Coords.). *Ética aplicada: novas tecnologias*. Lisboa: Edições 70, 2018, p. 9-27.

NILSSON, Nils J. *The quest for artificial intelligence: a history of ideas and achievements*. New York: Cambridge University Press, 2010.

RUARO, Regina Linden. Privacidade e autodeterminação informativa: obstáculos ao estado de vigilância? *Revista do Programa de Pós-Graduação em Direito da Universidade Federal do Piauí*, Teresina, v. 2, n.1, p. 41-60, jan./jun. 2015.

SARLET, Gabrielle Bezerra Sales; MOLINARO, Carlos Alberto. Questões tecnológicas, éticas e normativas da proteção de dados pessoais na área da saúde em um contexto de big data. *Direitos Fundamentais & Justiça*, Belo Horizonte, ano 13, n. 41, p. 183-212, jul./dez. 2019.

SARLET, Ingo Wolfgang. In: SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. *Curso de direito constitucional*. 10ª ed. São Paulo: Saraiva, 2021.

SARLET, Ingo Wolfgang. Fundamentos constitucionais: o direito fundamental à proteção de dados. In: MENDES, Laura Shertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otavio Luiz Rodrigues (Coords.). In: *Tratado de Proteção de Dados Pessoais*. Rio de Janeiro: Forense, 2021, p. 21-59.

SCHWAB, Klaus. *A quarta revolução industrial*. São Paulo: Edipro, 2016.

TANGARI, Gioacchino; IKRAM, Muhammad; IJAZ, Kiran; KAFAR, Mohamed Ali; BERKOVSKY, Shlomo. Mobile health and privacy: cross sectional study. *BMJ* 2021;373:n1248. Disponível em: <http://dx.doi.org/10.1136/bmj.n1248>. Acesso em: 27 mar. de 2023.

WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. *Harvard Law Review*, Cambridge, vol. IV, nº 5. pp. 193-220, dez., 15, 1890. Disponível em:

<https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf>. Acesso em: 26 mar. de 2023.

WITTGENSTEIN, Ludwig. *Tractatus Logico-Philosophicus*. 3ª ed. São Paulo: EDUSP, 2001.

WORLD HEALTH ORGANIZATION. *Health topics, e-Health*. Digital Health. Disponível em: <https://www.who.int/westernpacific/health-topics/e-health>. Acesso em: 16 out. de 2022.

7. UM ESTUDO SOBRE INTELIGÊNCIA ARTIFICIAL E OS RISCOS PARA A SAÚDE DAS CRIANÇAS: PERCEPÇÕES INTERNACIONAIS NA UNICEF E NA WEF

A STUDY ON ARTIFICIAL INTELLIGENCE AND RISKS TO CHILDREN'S HEALTH: INTERNATIONAL PERCEPTIONS AT UNICEF AND WEF



<https://doi.org/10.36592/9786554600552-07>

Lucas Reckziegel Weschenfelder¹

RESUMO

O texto apresenta uma síntese das iniciativas relacionadas às aplicações de inteligência artificial, e seus riscos para a saúde das crianças, em sede de UNICEF e de WEF.

Palavras-chave: Crianças. Inteligência Artificial. Saúde. UNICEF. WEF.

ABSTRACT

The article has a presentation regarding the recent initiatives in UNICEF and WEF, destined to study artificial intelligence and the risks of their use to the health of children.

Keywords: Children. Artificial Intelligence. Health. UNICEF. WEF.

INTRODUÇÃO

Todo exercício de abstração tem origem na "possibilidade ôntica" de se compreender o mundo de alguma maneira, e o que nele, a princípio, ocorre. Tradicionalmente, um exercício de abstração-compreensão aliançava-se à condição de ser da humanidade. A linguagem, o sujeito, o mundo, a *praxis*, são institutos que jogam à humanidade uma obrigação de refletir sobre si própria e, no caso, sobre as suas criações, as quais espelham as suas faces multifacetárias. Há aqueles que dizem que essa "possibilidade ôntica" está deixando ser característica única da

¹ Doutorando em Direito na Pontifícia Universidade Católica do Rio Grande do Sul. Advogado. Lattes: <http://lattes.cnpq.br/3929645670502613>. E-mail: lucasweschen@yahoo.com.br.

humanidade (TEIXEIRA, 2010, p. 108-110). O que se denomina de Inteligência Artificial (I.A.), considerando as diversas espécies e funcionalidades existentes, e em desenvolvimento, representa um novo capítulo histórico que, a depender das direções a que se vinculará, poderá resultar em uma ressignificação do “que é o ser”, e do Ihe constitui, em seu mundo prático, atento às conjunturas estruturantes da moral, da ética, do político, do econômico, do jurídico etc., que condensam sentidos complexos, que alimentam, e são alimentados, pelo social, em uma dinâmica de reciprocidade. Nessas asserções, com aparentes ares de generalidade, encontra-se um questionamento arendtiano, um tanto simples, porém, de difícil redarguição, caracterizado por: sabemos o que estamos fazendo? Nos compreendemos no nosso agir? Quais são os nossos objetivos? Quais as prognoses? Quais são os riscos de nossas ações? E quando sabemos que sabemos, qual a melhor postura a ser articulada?

Essas indagações acendem um alerta, que pode ser deslocado para os mais diferentes segmentos, em uma leitura macro, ou micro. Na hipótese, pretende-se ingressar em uma partícula normativa afeita à Inteligência Artificial (I.A.), no que diz em seu desenvolvimento, relacionado à utilização para e com crianças, dado que, se uma das maldições da condição humana é pensar no amanhã, vivendo no hoje, com um olhar jurídico-normativo, proteger, garantir e promover o bem-estar das crianças no presente, significa agir com um cuidado focado em direcionar as contingências do destino para um determinado lugar, aspirando-se um bem.

O Direito, vinculado à Teoria dos Direitos Humanos e Fundamentais, possui um compromisso em modular os processos socializados para finalidades justas, em que a dignidade da pessoa seja resguardada, em todo o seu processo de constituição, que se inicia na infância, na locução de proteção integral e do melhor interesse. Interessa-se em verificar, com uma revisão documental, algumas das reflexões que estão sendo organizadas, referentes aos riscos do emprego de I.A., para a saúde das crianças. Ingressar nessa temática suscita, no mínimo, pistas para encontrarmos respostas, ainda que inacabadas, para os questionamentos acima elencados.

No particular, objetiva-se trazer um recorte às prognoses, riscos e indagações da instrumentalização de Inteligência Artificial, à saúde das crianças, em especial,

em esfera internacional, optando-se pela iniciativa presente na *United Nations International Children's Emergency Fund* (UNICEF), e com a *World Economic Forum* (WEF).

O método de abordagem utilizado caracteriza-se por ser o hermenêutico, partindo-se de premissas que se consubstanciam no problema, o qual é desenvolvido no jogo da tradição, e da abertura para o mundo. Enquanto método de procedimento, emprega-se o monográfico. O presente trabalho foi realizado com apoio da PUCRS através do Programa de Excelência Acadêmica – PROEX – CAPES.

1 DA PROTEÇÃO INTEGRAL ANALÓGICA À TRANSIÇÃO PARA O DIGITAL

A proteção jurídica das crianças representa um esforço histórico que, paulatinamente, vem se consolidando. Desde horizontes atrelados à vulnerabilidade, até o fomento a um processo e desenvolvimento da pessoa, balizado por diretrizes atreladas ao potencial de emancipação. No Brasil, a Constituição de 1988 prevê uma estrutura de proteção integral (CUSTÓDIO, 2008, p. 32). Estado, família e sociedade são responsáveis pelo bem-estar das crianças.

No plano internacional, por exemplo, com a *Convention on the Rights of the Child*, das Nações Unidas, antecipa-se, no art. 3º, que, todas as ações concernentes às crianças, inicializadas pelo poder público, ou poder privado, devem se orientar pelo “[...] *the best interests of the child shall be a primary consideration*” (ONU, 1989, p. 3). Dita locução encontra-se registrada no art. 14, *caput*, da Lei 13.709/2018, legislação brasileira, com pertinência temática, dizendo-se que, “*o tratamento de dados pessoais de crianças [...] deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente*”, densificando a proteção de dados pessoais, no Brasil, recentemente reconhecida, em texto constitucional, como um direito fundamental (art. 5º, LXXIX) (BRASIL, 2022, 2018) (SARLET, 2020) (MOLINARO; SARLET, 2019) (ALBERS, 2016)².

² Não se olvida das diferenças históricas e regionais, relacionadas ao processo de constituição de uma compreensão e validação, jurídica-normativa, e social-normativa, da proteção da criança (e do adolescente). No Brasil, em rápida síntese, nota-se um amplo período de não reconhecimento, de criminalização, de utilização de mão de obra infantil etc., que se incorporava, dogmaticamente, na doutrina do ‘menor’, e da ‘situação irregular’ (para ficar, somente, no século XX).

Pensar o desenvolvimento tecnológico, pontualmente, aquele relacionado à digitalização e I.A., e seus potenciais riscos à saúde das crianças, não se imprime simplesmente atrelado à elementos teórico-práticos reflexivos, mas, enquanto dever, em especial, considerando-se os termos dos Direitos Humanos e Fundamentais, construídos, e em construção, destinados a garantir o bem-estar das crianças. Esse dever, a propósito, tem respaldo, igualmente, no Pacto Internacional sobre os Direitos Econômicos, Sociais e Culturais (BRASIL, 1992), local em que se estabelece o comprometimento dos Estados em reconhecer e a garantir o direito de todas as pessoas a gozar do melhor estado de saúde física e mental possível de atingir, havendo-se a obrigação dos Estados Parte de tomarem medidas para assegurar o pleno exercício de tal direito (art. 12º, 1. 2.).

Não é por acaso, porquanto, que, variadas organizações internacionais, que se ocupam de maturar normativas relacionadas aos direitos humanos, vêm dando atenção ao tema, como, a saber, a UNICEF (2022, 2021), e nos documentos da *World Economic Forum* (2022). Considerando o recorte para o texto, no que diz ao emprego de I.A., para e com crianças, e os riscos de tal desenvolvimento tecnológico à saúde, em sua dimensão multidimensional, remonta ser impreterível observar o que está sendo condensado sobre a matéria, em tais documentos internacionais, bem como seus diálogos com as esferas nacionais, e acadêmicas.

2 DA PROTEÇÃO DA CRIANÇA E DE SUA SAÚDE EM SEGMENTOS DE APLICAÇÕES COM INTELIGÊNCIA ARTIFICIAL – UM OLHAR DO CENÁRIO INTERNACIONAL

A Organização para a Cooperação e Desenvolvimento Econômico (OCDE), no documento nomeado de *Recommendation of the Council on Artificial Intelligence* (2019), utiliza o conceito de Inteligência Artificial (I.A.), no sentido de ser um sistema baseado em máquina que pode, para e em um determinado conjunto de objetivos definidos pelo homem, realizar previsões, recomendações ou decisões que influenciam ambientes reais ou virtuais, projetado para operacionalizar-se consoante um nível variado de autonomia. A mesma organização internacional incorpora a concepção de ciclo de vida da Inteligência Artificial, envolvendo-a em quatro etapas: i) design, dados e modelos, que é uma sequência que depende do

contexto, abrangendo planejamento, projeto, coleta e processamento de dados, bem como construção de modelo; ii) verificação e validação; iii) implantação; e iv) operação e monitoramento. Essas fases, geralmente, ocorrem de maneira iterativa e não são, necessariamente, sequenciais. Antecipa-se, ainda, que, a decisão de retirar um sistema de I.A. de funcionamento pode ocorrer a qualquer momento, durante a etapa de operação e de monitoramento.

Não se cita a referida iniciativa intergovernamental, para validar ou aceitar concepções que vêm sendo incorporadas, de modo semelhante, no cenário jurídico nacional, e internacional. Trata-se, somente, de uma forma de iniciar a seção, lançando a generalidade e a complexidade da matéria, e a sua relevância, no caso, para o Direito, e, ao mesmo tempo, situando-se que, na Recomendação, não há uma diretriz específica, no tocante a relação da criança, com a I.A. Tem-se ciente que, a iniciativa visa apresentar padrões normativos para a I.A., mas, ao mesmo tempo, é possível, com isso, visualizar, ao menos, um indício de que, a criança, nesse espaço, não é, necessariamente, 'objeto central' de proteção e reflexão, abrindo-se espaço, por isso, para estruturas setoriais, mesmo que assente uma defesa para a realização de uma I.A. *Human-centred*, fundada e orientada por percepções de *fairness* (1.2.)³. Passa-se para uma ligeira leitura sobre a iniciativa em sede de *United Nations International Children's Emergency Fund* (UNICEF), e sua reivindicação internacional para uma *children-centred A.I.*

³ 1.2. Human-centred values and fairness a) AI actors should respect the rule of law, human rights and democratic values, throughout the AI system lifecycle. These include freedom, dignity and autonomy, privacy and data protection, non-discrimination and equality, diversity, fairness, social justice, and internationally recognised labour rights. b) To this end, AI actors should implement mechanisms and safeguards, such as capacity for human determination, that are appropriate to the context and consistent with the state of art. Tradução livre: valores e justiça: a) Os atores envolvidos com I.A. devem respeitar o Estado de Direito, os direitos humanos e os valores democráticos, durante todo o ciclo de vida do Sistema de I.A. Estes incluem Liberdade, dignidade e autonomia, privacidade e proteção de dados, não discriminação, diversidade, igualdade, equidade, justiça social e direitos trabalhistas reconhecidos internacionalmente.; b) Para isso, devem implementar mecanismos e salvaguardas, como a capacidade para determinação humana, que sejam apropriados ao contexto, e consistentes ao estado da arte na matéria.

2.1 REGISTROS DE CUIDADOS RELACIONADOS À I.A. E CRIANÇAS EM SEDE DE UNITED NATIONS INTERNATIONAL CHILDREN'S EMERGENCY FUND (UNICEF)

Importa-se em considerar, o dito acima, para correlacionar as observações sumarias, com os trabalhos realizados pela *United Nations International Children's Emergency Fund* (UNICEF), que, por sua característica, adentra em espaços ainda em processo de constituição, quando pensando-se na I.A., e as crianças, sabendo-se, de suas próprias percepções, que, "*Most of the technologies that exist are not made with children in mind*" (UNICEF, 2021, p. 11).

No *Policy guidance on AI for children*, publicado pela UNICEF, em 2021, reflete sobre como os sistemas de I.A. estão, fundamentalmente, transformando o mundo, e os seres humanos, afetando, de modo substancial, a presente e as futuras gerações 'de crianças'. Os sistemas de I.A. vêm sendo incorporados em muitas atividades, que, direta, ou indiretamente, relacionam-se com a infância, e com o ator protagonista desse período de formação da personalidade, tal qual, a 'criança'. A aludida tecnologia encontra-se embebida em brinquedos, em assistentes virtuais, videogames e, também, em modalidades de *chatbots* que, contextualmente, 'relacionam-se' com as crianças.

Os algoritmos, igualmente, influenciam, mediante recomendações, os tipos de vídeos a serem vistos, o conteúdo da leitura, qual música escutar, e as formas de constituição de relações de amizade, no ambiente digital e, portanto, no social-analógico. Ainda, o documento chama a atenção à massiva inserção de aplicações de I.A., em sistemas de governança dos Estados, vinculados a redes de bem-estar social, relacionadas à saúde, à educação, à benefícios sociais envoltos a proteção da família (e de seus membros), que estão, cada vez mais, sendo organizadas com o emprego de sistemas de I.A., com leituras e decisões automatizadas⁴.

⁴ Cita-se, para exemplificar, o caso holandês, da cidade de Rotterdam (*Rotterdam's risk scoring system*). Refere-se a esse caso, pois, para além de ser originado em ambiente europeu – que vem avançando em preocupações relacionadas à regulação de aplicações de I.A. –, verifica-se, no estudo referenciado, que o Estado forneceu, parcialmente, após o envio de FOIAs (*freedom of information requests*), dados, modelos e metodologias empregadas, de modo a ser conferida, em teste próprio, as características do sistema, e seus já constatados riscos aos direitos humanos das pessoas atingidas. O que Rotterdam negou-se a fornecer, foi, essencialmente, os dados 'originais' dos cidadãos, utilizados no *score system* objeto de estudo. LIGHTHOUSE REPORTS. Suspicion machines methodology: a detailed explainer on what we did and how we did it. Disponível em:

Para além de tais riscos, não se ignora os benefícios, e potenciais benesses, de sistemas de I.A., para o auxílio no desenvolvimento das crianças. Inclusive, a própria UNICEF registra que vem empregando tais tecnologias, de modo a aperfeiçoar sua estrutura interna de programação, inserida em mapeamentos de conectividade digital em escolas, e na arquitetura preditiva relacionada a propagação de doenças, e elevação de constatações eficientes, no tocante a estimativa da pobreza, nesses cenários (UNICEF, 2021, p. 7). Aliás, aceita-se a validade de que, os sistemas de I.A. poderão ser de alta ajuda na estruturação de inovações, pensadas a partir dos *Sustainable Development Goals* – 2030, sem, contudo, olvidar, novamente, dos riscos de tais atividades, considerando-se que tais tecnologias podem operar sem ser notadas, e em grande escala, parâmetros tais que fazem necessária uma reflexão sobre o desconhecido, sobre o repensar as percepções normativas relacionadas à dignidade, e suas correlações com sentidos envoltos à noções de autonomia e agência humanas. Imperativa, porquanto, uma análise jurídica a partir de variadas frentes, em especial, no cenário internacional – que não imprime uma preocupação atenta a essa camada jushumana -, e sabendo-se que, “[...] *whatever is known about how children interact with and are impacted by AI is just the start. The disruptive effects of AI will transform children’s lives in ways we cannot yet understand, for better or worse*”⁵ (UNICEF, 2021, p. 7).

É justamente a partir de tais pressupostos que, a UNICEF reivindica o pensar um aparato envolto a uma *child-centred AI*, incorporando nove requerimentos complementares. Refere-se ao 1) Apoiar o desenvolvimento e o bem-estar das crianças (“deixe a I.A me ajudar a desenvolver todo o meu potencial”); 2) Garantir a inclusão de e para as crianças (“incluir a mim e aos que estão ao meu redor-comigo”); 3) Priorizar a justiça e a não discriminação para as crianças (“a I.A. deve ser para todas as crianças”); 4) Proteja os dados pessoais e a privacidade das crianças (“garanta minha privacidade em um mundo de I.A.”); 5) Garantir a segurança das crianças (“preciso estar seguro no mundo da I.A.”); 6) Forneça transparência,

<https://www.lighthousereports.com/suspicion-machines-methodology/>. Acesso em: 21 de abril de 2023.

⁵ Tradução livre: tudo o que se sabe sobre como as crianças interagem e são afetadas pela IA é apenas o começo. Os efeitos disruptivos da IA transformarão a vida das crianças de maneiras que ainda não compreendemos, para o bem ou para o mal.

capacidade de explicação e *accountability* para as crianças (“preciso saber como a IA me afeta. Você(s) precisa(m) ser responsáveis e responsabilizados por isso”); 7) Capacitar governos e empresas com conhecimento sobre I.A., e direitos das crianças (“você deve saber quais são meus direitos e assim defende-los”); 8) Preparar as crianças para o desenvolvimento presente, e futuro, em I.A. (“se eu estiver bem preparado agora, posso contribuir para uma I.A. responsável no futuro”); 9) Criar um ambiente favorável e inclusivo (“torne possível que todos contribuam para a uma *child-centred AI*”).

Recortando-se o assunto, especificamente, para os direitos das crianças e I.A., em uma preocupação com a saúde, nota-se, na seção “*target audience*”, do documento internacional em leitura, que, visa-se chamar a atenção para além do Estado, mas, de empreendimentos que forneçam produtos e serviços *AI-enabled*, como plataformas de mídia social, fornecedores de tecnologia para a educação, e sistemas de diagnóstico na área da saúde. Emprega-se uma ampla concepção de ‘saúde’, como aquela prevista na Constituição da Organização Mundial da Saúde, a qual atesta que, a “[...] saúde é um estado de completo bem-estar físico, mental e social, e não apenas a ausência de doença ou enfermidades” (BRASIL, 1948), e utiliza-se, também, o parâmetro etário da Convenção sobre os Direitos da Criança, da ONU, que considera criança, toda pessoa que possui menos de dezoito anos.

Divide-se a abordagem em três esquemas jurídico-normativos (extraíndo-se, tal divisão, da Convenção sobre os Direitos da Criança, da ONU) incluindo uma percepção envolta a proteção (*protection*), uma relacionada a elemento de provisão (*provision*), e outra de participação (*participation*). Com a proteção, destaca-se o direito contra qualquer tipo de discriminação, abuso ou forma de exploração, adicionalmente à privacidade e à proteção aos dados pessoais. Coloca-se um cuidado com espaços e mecanismos, formais e informais, institucionais ou sociais, em que a criança seja protegida, ouvida e seriamente considerada, em casos de violação aos seus direitos. No que diz à camada provisão, abarca-se o direito a serviços, a criação de habilidades e recursos que garantam à criança sua existência, e o desenvolvimento de seu potencial, à vista de parâmetros de igualdade de oportunidades, e de que toda a criança possui a *fair chance*. Coloca-se como eixos de tal parâmetro, o direito a saúde, a educação, a informação, ao descanso, ao lazer,

e ao de brincar. No que diz à matéria de participação, antecipa-se o direito de as crianças de livremente expressarem as suas opiniões, em todos os assuntos que lhes digam respeito, sendo-as seriamente consideradas, e ratifica-se que, a aproximação jurídico-normativa empregada é aquela baseada na linguagem dos Direitos Humanos das Crianças, e não em anteriores horizontes relacionados a *welfare approach*, em que se reconhece as crianças como seres humanos vulneráveis, passivos e necessitados (objeto de cuidado e caridade), em vez de se reconhecer as crianças como seres humanos com dignidade, agência e protegidos por uma distinção de direitos e prerrogativas.

São com esses eixos, reinterpretados, vasculhando-se o melhor interesse da criança, que o documento amplia um tratamento jurídico-normativo, de uma *children-centred AI*, buscando-se um comprometimento pelos atores públicos e privados, de modo a se trazer um ambiente social, biológico, psíquico e tecnológico saudável, para a primeira geração que "*will never remember a time before smartphones*", e que estará, inevitavelmente, impregnada, profundamente, por riscos atribuídos pela divisão digital, automação do trabalho, preocupada com proteção de dados pessoais e com a privacidade de formas inéditas, que caracterizam a atual sociedade, na qual, a propósito, ainda não se tem uma robusta noção sobre, e dos reais riscos de tecnologias baseadas em I.A., para as crianças (UNICEF, 2021, p. 20).

Complementando-se a observação, em outro momento, visualiza-se as diferenças contextuais e interseccionais de cada criança (e de sua respectiva família e/ou responsável), tendo em vista aspectos socioeconômicos, geográficos, culturais e, de condições pessoais mesmas, associadas ao desenvolvimento-evolução das crianças, em pontos físicos, cognitivos, emocionais, e psicológicos, que, inevitavelmente, impactam a relação da criança, com tecnologias baseadas em I.A. Procura-se colocar como objeto de reflexão, exatamente, as interações entre uma tecnologia I.A., e a criança, que pode ocorrer de maneira multifacetária, de forma direta, e indireta (mesmo os sistemas que não são projetados para 'interagir' com as crianças, devem estar equipados, de certa forma, para essa interação) (UNICEF, 2021, p. 20).

No particular à saúde, a UNICEF (2021, p. 21) destaca que, em uma percepção estrita, de práticas médicas e de pesquisa, os sistemas de I.A. por já estão sendo

empregados para assistir em processos de diagnóstico, triagem e em via de recomendação de tratamentos. Isso é realizado, por exemplo, com as habilidades de I.A., instrumentalizadas com processamento de linguagem natural (PLN), que podem auxiliar em pesquisas, na leitura de vastos bancos de dados de saúde, de uma miríade de artigos científicos, e gerar sínteses que facilitem o desenvolvimento em pesquisa, e de tratamentos. Realça-se as novas tecnologias assistivas perpetuadas com I.A., como aquelas que poderão ser transplantadas para novas modalidades de aparelhos auditivos, cujo propósito encontra-se na facilitação da audição, isolando vozes singulares, em uma multidão, e filtrando-se ruídos descabidos.⁶

É possível apreender, ainda, uma cautela com aplicações inteligentes que vêm aperfeiçoando suas capacidades para contribuir como suporte emocional e psíquico para as crianças, sem embargo, ainda se mantendo como epistemologicamente, metodologicamente e, eticamente, questionáveis. Valida-se espaços para a sua incorporação, quando em ambiente altamente controlado, com supervisão de comitês de ética e de bem-estar, considerando situações existentes⁷, e em desenvolvimento. Coloca-se que, essas modalidades de I.A. 'emocionais' são incorporadas em produtos ou serviços, que sejam capazes de detectar humores, emoções e problemas de saúde psíquica em evolução, de modo a auxiliar a dinâmica familiar, com o apoio parental, além de assistir em mecanismos de 'regulação' de comportamento por meio de aprendizagem socio-emocional. Em tais projetos, resulta como mandatária a obrigação de garantir que, em casos delicados, as

⁶ Na seção em questão, cita-se o texto de Utermohlen, K. Applications of Artificial Intelligence for Hearing Loss, de 2018. Desde o período, muitos avanços ocorreram na área em questão, com a utilização de I.A, cujas aplicações variam desde adaptações a contextos, aprendizado de máquina, personalização do equipamento assistivo, de acordo com experiências passadas, do usuário, e de outros, constante em banco de dados empregado, aumentando-se, também, a autonomia da pessoa com deficiência auditiva, que poderá adaptar o sistema de forma simultânea, às eventuais recomendações realizadas pelo aparelho auditivo 'inteligente'. Destaca-se que, um dos principais benefícios desses novos sistemas, está para o aperfeiçoamento da memória, não em um sentido de 'aumento de capacidade cognitiva', mas, como resultado do que se denomina de "esforço para escutar (*listening effort*), pois a pessoa passa a poder se concentrar mais no conteúdo, e nas nuances em que está inserida, como em aulas, classes ou conversas informais. Cita-se dois exemplos: WIDEXPRO. Artificial Intelligence in our hearing aids, 2023. Disponível em: <https://www.widexpro.com/en/widex-technology/artificial-intelligence/>. Acesso em: 26 de abril de 2023. HEALTHYHEARING. Hearing aids with artificial intelligence, 2021. Disponível em: <https://www.healthyhearing.com/report/53168-Hearing-aids-artificial-intelligence-deep-learning-oticon>. Acesso em: 26 de abril de 2023.

⁷ Exemplifica-se com o Milli (AI-powered chatbot), de iniciativa do Hospital da Universidade de Helsinki (*mental health issues*), usado, majoritariamente, por maiores de 12 anos.

crianças sejam direcionadas aos suportes humanos, em condições online e offline (UNICEF, 2021, p. 21).

Dentro de um escopo de análise de risco, inclui-se como necessário um olhar constante aos possíveis prejuízos advindos de discriminações e exclusões sistêmicas e automatizadas. As limitações às oportunidades e ao desenvolvimento da criança, mediante predições analíticas e com perfilamento, podem ser graves, tanto em ambientes privados, quanto públicos. Por exemplo, análises estatísticas mediante *predictive modelling applications* podem (e são) empregadas com a finalidade de aperfeiçoar a alocação de recursos no orçamento público, voltados a serviços de saúde e cuidado. Esse trabalho é construído, no geral, mediante diferentes banco de dados (que, também, variam de acordo com cada país e suas características), que, por sua vez, já apresentam casos e critérios próprios ou construídos durante o processo, prévio ou contemporâneo.

Coloca-se como problemática a questão, à vista de que, os dados oriundos de sistemas públicos de bem-estar, informações médicas e, em vezes, judiciais (entre outros), podem, em seu *input*, estarem organizados de modo insuficiente e assistemático, pela própria infraestrutura governamental, em que cada órgão local, por exemplo, é capaz de estar trabalhando de forma e com critérios diferentes, sem diálogo interoperacional e coerente, o que, também, poderá causar falta de informações relevantes sobre determinadas áreas e cidadãos, ou, ainda, haver equívocos no material reportado e tratado. Isso significa uma problemática quanto aos riscos de se reforçar, senão amplificar, padrões históricos vinculados a discriminações e insuficiências sistêmicas, representando potenciais de violação aos direitos das crianças, em especial, aqueles relacionados à saúde (UNICEF, 2021, p. 22).⁸

É por isso que, associa-se o desenvolvimento de banco de dados, relacionado a dados de crianças, com um cuidado atento à diversidade, como expressão mesma de uma estrutura equânime de dados (incluindo-se preocupações aos dados de crianças de diferentes regiões, idades, etnicidade, cultura, e condição

⁸ Ver, para informações adicionais sobre a temática o trabalho em: UNICEF; THEGOVLAB. Responsible data for children training, 2022. Disponível em: <https://rd4c.org/articles/new-publication-responsible-data-for-children-releases-slides-for-self-guided-training/index.html>. Acesso em: 24 de abril de 2023.

socioeconômica), todavia, com explícitos cuidados ao excesso de tratamento, de modo a, realmente, ser possível proteger e beneficiar as crianças, nesses momentos. Em sistemas de saúde orientados por dados, (*data-driven health care*), a UNICEF (2021, p. 34-35) salienta que, o tratamento, curativo ou preventivo, não pode ser assistido, mediante leituras de dados e informações oriundos de contextos de adultos, uma vez que isso poderá gerar riscos desconhecidos à saúde da criança.

Em outro ângulo, antepõe-se uma preocupação em como refletir, e instituir práticas de I.A., que consigam concretizar, eficazmente, os direitos das crianças, em suas manifestações – de proteção, provisão e de participação. Em sua indivisibilidade, observa-se uma certa preponderância normativa contextual, embora ciente de que, em cada etapa, haja um necessário exame atento a um '*balance*' das medidas, instrumentos e finalidades (UNICEF, 2021, p. 31). No âmbito da saúde, essas práticas são recorrentes, e, pelo complexo interligado de assuntos e cuidados, reflete-se a imperatividade de se constituir, a cada momento, situações capazes de criarem parâmetros normativos ótimos, que respeitem a autonomia da criança⁹, a expertise médica e, ainda, novas manifestações relacionadas ao poder familiar, nesse particular.

Essas preocupações, colocadas sumariamente, abrem, cada qual, espaços para reflexões que não cabem no presente texto, tampouco encontram-se adequadas ao seu objetivo. Sem embargo, em nota conclusiva, verifica-se que, no documento em questão, visa-se aprofundar uma percepção atenta as iniciativas de aplicações com I.A., para com as crianças, em uma abordagem a partir da linguagem dos direitos humanos e fundamentais das crianças, que, inevitavelmente, deverá ser 'atualizada' aos novos desafios que já se apresentam, e aos futuros. Anota-se como apropriada a desenvoltura de uma concepção de I.A. responsável, a qual, no contexto de relações com crianças, deve ser balizada por uma postura de *fairness*, a qual não deve ser encarada como 'dada', mas, reconhecendo-se como cada medida poderá

⁹ Dentre os questionamentos copiados no documento em estudo, coloca-se como central (e com variados desdobramentos), justamente: For example, how can children's privacy and agency be best protected while collecting suficiente data on children for specific AI-based health interventions? Tradução livre: Por exemplo, como a privacidade e a agência das crianças podem ser melhor protegidas ao coletar dados suficientes sobre crianças para intervenções de saúde específicas baseadas em IA?.

afetar as crianças de maneiras diferentes, ainda mais, em contextos relacionados à saúde.

2.2 APLICAÇÕES DE INTELIGÊNCIA ARTIFICIAL E A PROTEÇÃO DE CRIANÇAS EM SEDE DE *WORLD ECONOMIC FORUM* (WEF)

Opta-se em discorrer, brevemente, sobre as iniciativas temáticas realizadas na *World Economic Forum* (WEF), de modo a acrescer os horizontes relatados a partir das posições tomadas na UNICEF. A organização internacional escolhida, ainda que seja objeto de críticas, é, todavia, um centro de influência mundial, em variados segmentos e atividades, não sendo diferente, no caso, no campo da I.A. Ressalta-se que, o documento em leitura torna-se por ser o designado *Artificial Intelligence for Children*, de 2022, o qual, a propósito, tem um destino e escopo limitado, tanto em termos materiais, quanto formais, no sentido de seus destinatários. A finalidade do documento revela-se em ajudar os empreendimentos privados a desenvolver tecnologias de I.A. confiáveis para crianças, de modo a assistir os pais, e eventuais responsáveis, na via de "*responsibly buy and safety use AI products*" (WEF, 2022, p. 3).

Há uma diretiva padrão no texto em comento, ao se pontuar que, as tecnologias de I.A., podem possuir impactos positivos na sociedade, e para as crianças. No entanto, tal perspectiva não há de ser utilizada como um algo exato, pois, as crianças podem ser objeto de negatividades e de riscos, colocadas pelas novas tecnologias de I.A., relacionadas à aspectos de vulnerabilidade, vieses, discriminação, cibersegurança, e, ainda, por ausência de acessibilidade, tanto 'interna', como 'externa'.

Da mesma forma que antecipado no documento da UNICEF, defende-se um desenvolvimento de I.A. *child-centred*, assim sendo incorporado, na origem, parâmetros envoltos à infância e às crianças. A inovação deve ser acompanhada de responsabilidade, que é classificada por representar noções de segurança, ética, transparência, justiça, acessibilidade e inclusão. Além de se pensar em aspectos específicos e contextuais das crianças, há de se ampliar o escopo para a própria atuação dos pais, e de responsáveis, nessas relações.

A WEF (2022) propõe uma chamada metafórica e de publicidade, com o acróstico "*putting children and youth FIRST*", em que o desenvolvimento de I.A. é observado a partir de seus requerimentos mandamentais, tais como, *Fair, Inclusive, Responsible, Safe, e Transparent*. Realiza-se uma aproximação, tendo em vista os horizontes de cada ator que, de maneira direta, ou indireta, é tido como responsável, na relação da criança, com uma ou mais tecnologias de I.A - *corporate decision-maker, member of a product team, parent or guardian*).

Para executivos, ou membros de times de desenvolvimento, apresenta-se um *C-suite checklist (Corporate users)*, em que, para se buscar uma *children-centred A.I.*, há de se pensar em *real-world guidance*, para auxiliar as iniciativas no ramo, desde o *design* básico dos produtos e serviços, inclusive para aqueles que, em um primeiro momento, não estarão destinados às crianças, uma vez que, não raro, é difícil prever quais deles acabarão sendo utilizados por elas, sendo essa prática uma regra padrão, vinculada a se buscar meios de mitigar potenciais riscos da tecnologia, para esse grupo.

Dita dinâmica é de particular importância para aqueles atores cujas funções estejam em desenvolver os serviços e produtos (*design, develop, and deploy*) de I.A., dos quais as crianças, provavelmente, irão ser usuárias. A responsabilidade desses atores inicia com a idealização do produto ou serviço, e prolonga-se para todo o ciclo de vida da tecnologia, em aperfeiçoamentos e aprendizados próprios (WEF, 2022, p. 4), em especial com aqueles que, de forma ampla, promovem profunda imersão cognitiva, emocional, e comportamental, na interação com a criança.

Os empreendimentos privados atuam de maneira insuficiente, nesse espaço, quando, deixam de i) apresentar ao usuário, a forma que a inteligência artificial é usada no serviço, ou produto ("*be transparente about the use of AI and why you are using it*"); quando ii) não criam um arcabouço detido para o enfrentamento de vieses, que podem ampliar ou perpetuar discriminações; iii) manipula-se a cognição/foco do usuário, de modo a impedir uma experiência atenta e válida, sobre a tecnologia, e seus riscos para a pessoa, como "*prototyping stages*"; e iv) apresenta problemas de privacidade, proteção de dados e de segurança, tanto para a criança, quanto em relação aos mecanismos que seus pais, ou responsáveis, podem utilizar, para assistir nesses contextos; salienta-se, nesse ponto, as diferenças regionais e

nacionais, de regulação, relevantes para considerar, em um tema com aspectos globais e locais.

Como instrumento para reverter tais situações, sugere-se as seguintes condições: i) implantar medidas consoante as propostas legais e regulatórias de cada setor, aliando-se aspectos nacionais e internacionais (como da *Electrical and Electronics Engineers IEEE code of ethics*, UNICEF entre outras). Reforça-se um compromisso com um sistema de classificação/rotulação (*labelling system*) adaptado às novas tecnologias de I.A.; realizar compromissos internos e externos, informando, igualmente, em linguagem acessível, todas as características essenciais sobre a tecnologia, e formas de se comunicar com a companhia, especialmente com indicadores aos pais e responsáveis das crianças. ii) criar um time de executivos e de desenvolvimento diverso, cometicistas, pesquisadores, especialistas em privacidade e proteção de dados, educadores, especialistas em desenvolvimento de crianças, psicólogos, designers e cientistas de dados; adiciona-se uma necessária colaboração com organizações sem fins lucrativos e abertura para trocas, com instituições de pesquisa focadas na área. iii) treinar, continuamente, o time de desenvolvedores de produtos e serviços, apontando a essencialidade de se criar tecnologias de I.A. responsáveis e confiáveis, dentro do escopo normativo de uma *child-centred A.I.*; iv) contribuir, publicamente, com os avanços e experiências realizadas no empreendimento, de modo a enriquecer possibilidades de regulação ou diretrizes regionais, nacionais e internacionais aplicáveis na área; em mais uma oportunidade, a WEF registra como imperativa a recepção de se utilizar v) sistemas de classificação/rotulação das tecnologias de I.A., de acordo com o potencial de impacto nos usuários (*risk approach*), informando-se todas as características essenciais do produto e do serviço, bem como mecanismos de atuação para que os usuários, crianças, pais e responsáveis, possam realizar escolhas informadas (WEF, 2022, p. 8).

Apropriado, ainda, apresentar uma síntese particular, sobre as diretrizes da WEF, para a formatação de um desenvolvimento responsável, durante todo o processo e ciclo de vida da tecnologia da I.A. (*product team guidelines*). A partir do referido acróstico FAIR, propõe-se uma *child-centred A.I.*, que encontra-se desde o projeto, pensado e constituído com o melhor interesse da criança, em tecnologias

especificamente destinadas à elas, ou, adaptando àquelas que, provavelmente, serão empregadas direta, ou indiretamente, em relações que afetem seus interesses e direitos.

O desenvolvimento de uma *child-centred A.I.*, nesse espaço, densifica-se com as seguintes noções. Desdobrando-se percepções de *Fair*, coloca-se que, o produto ou serviço, em sua integralidade, precisa estar atento para os riscos de danos, em aspectos de quebra de i) expectativa-confiança do usuário e dos pais ou responsáveis e, modelando-se consoante a dogmática de proteção de dados pessoais, quanto às reais informações fornecidas, e no próprio *design*, para que o procedimento de consentimento, explícito ou implícito, seja adequado. Em um segundo momento, ii) a mitigação de riscos deve ser acompanhada com uma estratégia constante e proativa de governança, que pode ser inspirada, a saber, nos questionamentos indicados no Berkley-Haas *ethics questions* (e outros), que exsurge em variados *frameworks* éticos: a) como a decisão tomada refletiria no espaço público?; b) o que aconteceria se todos fizessem isso?; c) se alguém fizer isso comigo, qual seria a minha reação?; d) o curso de ação proposto projeta um bom resultado?; e) o que o curso de ação proposto fará ao meu caráter, ou ao caráter da organização que faço parte?; f) o curso de ação proposto é consistente com meus valores e princípios defendidos, e, complementa-se, eles estão de acordo com o direito das crianças? (WEF, 2022, p. 15)¹⁰.

Há de se encarar os riscos identificados, não como erros, mas, como avanços a serem registrados e trabalhados. Nos testes e treinos com dados, um dos principais propósitos de mitigação, precisa ser voltado a observação comportamental do modelo em processo, e suas áreas com vieses, presentes, ou potenciais, respondendo-se, pelo menos, as indagações, advindas de, como o produto foi definido e medido, em seus vieses de I.A., como esses vieses foram corrigidos? E quais lacunas e benefícios foram descobertos desse processo de aperfeiçoamento? (WEF, 2022, p. 16).

¹⁰ Indica-se, ainda, os seguintes documentos: LUPI, Giorgia. Data humanism, the revolution will be visualized. D'IGNAZIO, Catherine.; KLEIN, Lauren. Data feminism.; DATA CAPITALISM, Data for Black Lives.

Relacionando-se ao esquema de *Inclusive I.A.*, registra-se uma preocupação com a acessibilidade de crianças com, e sem deficiência, em todas as suas expressões, físicas, mentais ou psíquicas, incluindo-se a linguagem da neurodiversidade. O idioma, a cultura e a classe social também são considerados, e fazem parte de uma preocupação essencial com uma forma de 'inclusão emocional' da I.A., de modo a se prevenir formas de exclusão, intencionais ou não intencionais. Esse aspecto, à vista de se estar pensando em relações da tecnologia, com crianças, apresenta-se em uma conduta preventiva de não se criar exclusões *by design*, com as quais as crianças, diferente de adultos, em vezes, não possuem uma capacidade cognitiva-emocional madura para compreender a questão, racionalizá-la de modo a entender que, eventual tecnologia não estava disponível para o seu parâmetro etário ou social-cognitivo, ou, ainda, que a tecnologia encontra-se em fase embrionária de desenvolvimento. Esses exemplos anunciam que, inadvertidamente, a tecnologia poderá causar danos graves à criança, em um sentido ainda não previsto, mas certo de que, em nuances distintas daquelas que, talvez, sejam motivo de influência 'excludente', realizada por tecnologia de I.A., em face de adultos (WEF, 2022, p. 17).

Ainda, antecipa-se como pressuposto, que, toda I.A. possui uma certa forma e modalidade de viés, que pode se dar em *bias in*, *bias out*, e em *bias internalized*. O viés em I.A. pode resultar em danos quando assume como inevitáveis determinadas atitudes, habilidades, capacidades e crenças, que influem na relação, direta ou indireta, com a criança. Quando a I.A. decide, em variadas conclusões, sobre uma pessoa, poderá estar reforçando ou ampliando discriminações, como as que já foram identificadas, por exemplo, com crianças com lábio leporino, em que filtros de câmeras não as reconheciam. Tais consequências podem ser nefastas na experiência humano-tecnologia, causando confusão na criança, e efeitos negativos para a sua saúde psíquica e moral, reforçando ou aprofundando experiências desagradáveis do passado.

Quando se avança para o aspecto de *Responsible A.I.*, tem-se como finalidade a confirmação do processo de internalização de responsabilidades, pela equipe desenvolvedora da I.A., tendo em vista os aspectos multifacetários das crianças. Essa diretriz antecipa uma postura de lucidez, no sentido de se ter ciente a ausência de conhecimento ou habilidades suficientes para avaliar, adequadamente, os riscos

de introduzir determinada tecnologia de I.A., para as crianças. Sucessivamente, observa-se como essa postura deve se revelar como uma tentativa constante de maturação, em todas as etapas da concepção da tecnologia, no *design*, planejamento, desenvolvimento e teste do produto, as quais devem ser justificados para além de elementos etários – que dizem algo, mas pouco – sobre as crianças, mas, avançando-se, em conjunto, com análises profundas dos estágios de desenvolvimento diversos que cada criança pode manifestar (exemplo: idade de 11 anos, com habilidade cognitiva de 15, com inteligência emocional de 10, e corpo de 14), além de se empregar as metodologias de ciência de dados que estejam atualizadas, ou sejam mais apropriadas a esse tipo de ação. Para chegar-se a estados ótimos, cada etapa deve ser objeto de análise conjunta, de uma equipe caracterizada pela interdisciplinaridade (WFE, 2023, p. 19).

Nesse paço, sugere-se a constituição de conselhos consultivos e de pesquisa, com participantes que representem a variabilidade dos público-alvo, margeando-se com as seguintes indagações: i) com o modelo de produto ou serviço de I.A., como foram verificados o estágio de desenvolvimento, e a idade, propriedades de adequação relacionadas a responsabilidade da tecnologia para com as crianças? ii) por que a I.A. foi incluída no produto? Como está a justificativa para a sua inclusão? Ela apresenta benefícios? Quais? iii) quando e com que frequência (e, se não), tem-se a atuação de pesquisadores e testes sobre o produto, incluindo-se crianças, pais/responsáveis, professores, e especialistas setoriais, para confirmar a adequação do 'estágio de desenvolvimento' e a 'idade'? iv) como o produto de I.A., confirma ou processa os *loops de feedbacks* para o usuário, pais/responsáveis, profissionais da educação (por exemplo), em futuras iterações, recursos e características da tecnologia, em tais relações?

Em proposições, recomenda-se a busca contínua por falhas, do produto, ou advindas de experiências do usuário (que podem ser situações e coisas distintas), incluindo-se as crianças em cada etapa do desenvolvimento da I.A. Mapear as áreas que apresentam mais riscos, focando-se em como pode-se mitigar e resolvê-las, bem como, quais as projeções de tais riscos, aceitando-se testes livres e contínuos. Analisar como os dados são tratados, quais, e em quais contextos. A I.A. permite ao usuário interagir com outras tecnologias e/ou pessoas? Como isso acontece? Há

segurança e mecanismos de *report*? Necessária a criação de processos que, com o tempo, construam uma convicção em torno do comportamento da tecnologia, e de suas habilidades de adaptação à cada circunstância, e criança destinatária da relação. Conclusivamente: a tecnologia de I.A. será capaz de ajustar seu comportamento baseando-se em sinais explícitos ou implícitos de estágio de desenvolvimento da criança (quais?), por exemplo, destreza física, habilidades cognitivas e linguísticas? As crianças, pais ou responsáveis serão capazes de corrigir eventual resultado advindo da I.A., se decisões incorretas impactarem a forma de relação, mediante, por exemplo, leitura equivocada sobre o estado de desenvolvimento da criança? Se sim, como? (WEF, 2022, p. 20).

Em diretrizes destinadas a uma *Safe I.A.*, projeta-se elementos preocupados com os estados físicos, mentais, psíquicos e emocionais das crianças. Criar um ambiente seguro, ainda em relações com tecnologias de I.A., deve integrar todo o planejamento do produto ou serviço inteligente. Inclui-se, a saber, para além de razões sociais e biológicas, fundamentos neurocientíficos, tais como o ainda em desenvolvimento córtex pré-frontal, cujos resultados podem representar, pelas crianças, ações impulsivas, ausência de parâmetros capazes de preverem consequências, e ausência de entendimento-experiência, em contextos nos quais possam estar sendo manipuladas, tanto na relação direta com a I.A., ou quando esta esteja sendo instrumentalizada por terceiros em seu prejuízo (WEF, 2022, p. 21).

Salienta-se que, para o desenvolvimento de uma tecnologia de I.A., há de se ter cuidado com usos desviantes de suas funcionalidades originárias. É claro que se torna impossível prever todas as potenciais malversações, no entanto, faz parte do trabalho de criação e desenvolvimento, refletir e buscar impedir formas futuras de usos maliciosos e intencionais da tecnologia, ou, instrumentalizações 'obliquas'. Uma condição preventiva e de cuidado, não somente concretizada pelo empreendimento, mas, em conjunto com os pais/responsáveis pela criança, precisa estar afinada, incidindo desde à origem do produto ou serviço, até o acompanhamento em processos de aperfeiçoamento (ex.: *designs* causadores de possíveis vícios; manipulações; riscos de contato com terceiros; conteúdo discriminatório e abusivo; leituras e conclusões demográficas desconformes;

proteção de dados pessoais e cibersegurança; formas de reportar e identificar esses cenários) (WEF, 2022, p. 21).

Anotando-se recomendações quanto à uma *Transparent I.A.*, a WEF (2022, p. 23) reforça o seu comprometimento com a idealização de um *AI labelling system*, para além de se respeitar regulações estatais ou interprivadas. Sobreleva-se seis categorias que, em síntese, precisam ser desenvolvidas no eixo em apreço. i) idade: para qual idade ou estado de desenvolvimento o produto ou serviço de I.A. será recomendado? Quais materiais a I.A., potencialmente, poderá expor ao usuário, e como esse material estará apropriadamente determinado de acordo com a idade, ou estado de desenvolvimento da criança? ii) acessibilidade: como o produto ou serviço inteligente estará acessível para as crianças de diferentes idades, capacidades e incapacidades, considerando os múltiplos contextos culturais e educacionais, por exemplo? A I.A. foi desenvolvida com parâmetros ótimos de inclusão? iii) câmera e microfone: se existentes câmera e/ou microfone no dispositivo, como estes estão apostos? É possível ligar e desligar? Ou haverá uma constante gravação do usuário? iv) rede/networks: o produto permite ao usuário/criança socializar com outras pessoas (quais tipos?) em um sistema de jogos ou de mídias sociais? Como o produto auxilia na criação de um ambiente saudável e seguro? Como a regulação privada, do próprio produto disponibilizado, está promovendo uma atmosfera válida e de confirmação de que a criança não estará em situações de risco? v) uso da I.A.: como o produto emprega a tecnologia de I.A.? Como o dispositivo poderá beneficiar a criança e a sua experiência? Quais os riscos de tal tecnologia? vi) uso de dados pessoais: como os dados pessoais da criança estão sendo tratados? Quem guarda as informações? Há compartilhamento? Se sim, com quem, e quais as garantias que este terceiro apresenta? Em qual local os dados pessoais estão armazenados, e como o banco de dados está protegido? Como a tecnologia e o produto se comunica com a criança/pais/responsável, considerando o tratamento de dados pessoais realizado e os eventuais futuros tratamentos? (WEF, 2022, p. 24).

Põe-se em diálogo a transparência, como pressuposto para a criação de relações de confiança, entre a criança, pais e/ou responsáveis e a tecnologia. Procura-se mostrar a relevância de uma adequada estrutura desde o dia 1, até o dia 100, mesmo durante atualizações e funcionalizações que, originalmente, não

estavam disponíveis no sistema de I.A. Os pais e responsáveis devem estar, como a criança, no centro de cuidados do desenvolvimento da tecnologia. Há de se ter uma comunicação clara e transparente entre os riscos, os limites e as estruturas que os pais/responsáveis podem empregar para aprender ou, ainda, assistir a criança no uso da tecnologia, dentro de suas disposições de poder familiar. Sugere-se, para determinadas tecnologias, uma organização de *notice*, o qual deverá ser encaminhado diretamente aos pais, quando as fronteiras pré-estabelecidas forem violadas, seja pela própria criança, amigo, ou eventuais terceiros em que esteja em relação (WFE, 2022, p. 24-25).

A WFE (2022, p. 25-26) reafirma o seu horizonte, relacionado com uma postura *risk approach* de desenvolvimento e regulação de I.A, e, ainda, apresenta a condição de que, os graus de riscos podem ser variáveis, de acordo com a evolução tecnológica, contextos, destinatários e inovações quanto a segurança ou propósitos. Recomenda-se estabelecer as propriedades mais conservadoras e restritivas, como *default*, no sistema de I.A. (de privacidade, tratamento de dados, compartilhamento, acesso etc.), e mecanismos de alertas de possíveis consequências, caso o usuário (criança/pais/responsáveis) decida modificar a configuração.

Para complementar o sistema de *labelling* e de *risk approach*, sugere-se, como expressão do poder familiar dos pais (e de poderes transitórios de responsáveis) uma condição de competências digitais, como elemento essencial de proteção aos direitos das crianças. A saber: i) idade – para qual idade a tecnologia é destinada? Acesse o *website* do produto e compreenda as suas características; solicite informações no canal de contatos de atendimento; ii) acessibilidade: quais as necessidades da criança, e seu estado de desenvolvimento? como a tecnologia se comunica à essas características? Estude e leia opiniões sobre a tecnologia; iii) sensores: saiba se a tecnologia possui sensores, como eles funcionam e quais dados são tratados; conheça e reconheça os riscos e o tipo de relação que a criança possui com a tecnologia; iv) *networks*: pesquise se a criança possui acesso a redes sociais ou outras modalidades de socialização com terceiros, mediante o uso da tecnologia, como em jogos online ou fóruns; v) uso da I.A.: fique ciente se a tecnologia produz mecanismos de recomendações ou sugestões sobre as situações em que a criança esteja envolvida; saiba se a criança pode ser gravemente impactada por essas

recomendações, e seu conteúdo, e eventuais manipulações, tanto própria, da tecnologia, como oriundas de eventuais terceiros; vi) tratamento de dados pessoais: compreenda se a tecnologia realiza o tratamento de dados pessoais, seus, da família e de seu(s) filho(s); fique ciente de quais dados pessoais são tratados, e, no mínimo, conheça os principais riscos de tal relação tecnológica (WEF, 2022, p. 32).

Trata-se de uma síntese das diretivas apresentadas pela WEF, as quais, ainda que destinadas aos empreendimentos privados, desenvolvedores de aplicações de I.A., pais e responsáveis, imprimem-se com ideias interessantes, ou receptivas de propostas de regulações 'estatais', oriundas do cenário europeu, acadêmicas e de instituições de pesquisa, e de recomendações diversas presentes em iniciativas de outras de organizações internacionais.

CONCLUSÃO

De nota conclusiva, é viável referir que, ambos os documentos, apesar de suas distinções, visam orquestrar, no mínimo, um movimento internacional voltado a uma *child-centred A.I.*, incorporando linguagens e diretrizes sedimentadas em aspectos de propostas estatais, presentes em reflexões acadêmicas, de institutos de pesquisa, e de iniciativas de outras organizações internacionais, ou organizações sem fins lucrativos, atuantes na área.

A iniciativa advinda da UNICEF, expõe um diálogo mais amplo, destinado aos Estados, entes privados e demais organizações internacionais. De outro, com a WEF, registra-se diretrizes específicas (que não foram, exaustivamente, comentadas), aos empreendimentos privados, bem como, para os pais/responsáveis pelas crianças.

A dogmática da proteção integral e do melhor interesse da criança, e seus reflexos normativos e simbólicos, estão em trânsito para proteger as novas camadas da pessoa-criança, no ambiente digital e analógico, impactado por novas e imprevisíveis tecnologias de I.A. Extrai-se que, medidas interconectadas e multilaterais são imperativas, de modo a influir, de modo cooperativo, todos os atores que atuam na área.

Uma análise que se quer crítica, em relação aos materiais descritos, ficará para outro momento, dado que, o propósito do texto está conexo a um projeto

particular, de, inicialmente, mapear as iniciativas internacionais, no que diz à proteção aos direitos das crianças em relações tecnologias de I.A., e seus riscos para a saúde.

REFERÊNCIAS

ALBERS, Marion. A complexidade da proteção de dados. Direitos fundamentais & justiça, Belo Horizonte, n. 35, p. 19-45, jul./dez. 2016.

ALI, Safinah. DIPAOLA, Daniella.; LEE, Irene.; SINDATO, Víctor.; KIM, Grace.; BLUMOFE, Ryan.; BREAZEL, Cynthia. Children as creators, thinkers and citizens in AI-driven future. Computers and educations: artificial intelligence. N. 2, 2021.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília: Presidência da República, 2022. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 30 out. 2022.

BRASIL. Emenda Constitucional nº 115, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm#ar. Acesso em: 11 out. 2022.

BRASIL. Decreto nº 591, de 6 de julho de 1992. Atos Internacionais. Pacto Internacional sobre Direitos Econômicos, Sociais e Culturais. Promulgação. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d0591.htm. Acesso em: 17 out. 2022.

CUSTÓDIO, André. Teoria da proteção integral: pressupostos para compreensão do direito da criança e do adolescente. Revista do Direito, n. 29, p. 22-43, 2008.

ECPAT.; INTERPOL.; UNICEF. Disrupting harm in Kenya: evidence on online child sexual exploitation and abuse. Global Partnership to end violence Against children. 2021. Disponível em: <https://www.end-violence.org/sites/default/files/2021-10/DH%20Kenya%20Report.pdf>. Acesso em: 24 out. 2022.

HEALTHYHEARING. Hearing aids with artificial intelligence, 2021. Disponível em: <https://www.healthyhearing.com/report/53168-Hearing-aids-artificial-intelligence-deep-learning-oticon>. Acesso em: 26 de abril de 2023.

LIGHTHOUSE REPORTS. Suspicion machines methodology: a detailed explainer on what we did and how we did it. Disponível em:

<https://www.lighthousereports.com/suspicion-machines-methodology/>. Acesso em: 21 de abril de 2023.

MARKAUSKAITE, Lina.; et. al. Rethinking the entwinement between artificial intelligence and human learning: what capabilities do learners need for a world with AI? *Computers and education: artificial intelligence*. n. 3, 2022.

MOLINARO, Carlos Alberto.; SARLET, Gabrielle Bezerra Sales. Questões tecnológicas, éticas e normativas da proteção de dados pessoais na área da saúde em um contexto de big data. *Direitos Fundamentais & Justiça*, ano 13, n. 41, p. 183-212, jul./dez., 2019.

OECD. Recommendation of the Council on Artificial Intelligence, adotada em 2019. Disponível em: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>. Acesso em: 19 de abril de 2023.

ONU. Convention on the rights of the child, 20 november 1989. Human Rights Instrument. Disponível em: <https://www.ohchr.org/sites/default/files/crc.pdf>. Acesso em: 24 out. 2022.

SARLET, Ingo Wolfgang. Proteção de dados pessoais como direito fundamental na constituição federal brasileira de 1988: contributo para a construção de uma dogmática constitucionalmente adequada. *Direitos fundamentais & justiça*, Belo Horizonte, ano 14, n. 42, p. 179-218, jun./jan. 2020.

SU, Jiahong.; YANG, Weipeng. Artificial intelligence in early childhood education: a scooping review. *Computador and education: artificial intelligence*, n. 3, 2022.

TEIXEIRA, José de Fernandes. *A mente pós-evolutiva: a filosofia da mente no universo do silício*. Petrópolis: Editora Vozes, 2010.

UNICEF. Investigating risks and opportunities for children in a digital world: a rapid review of the evidence on children's internet use and outcomes. Florence: UNICEF, 2021. Disponível em: <https://www.unicef-irc.org/publications/pdf/Investigating-Risks-and-Opportunities-for-Children-in-a-Digital-World.pdf>. Acesso em: 16 out. 2022.

UNICEF. Policy guidance on AI for children. New York: UNICEF, 2021.

WIDEXPRO. Artificial Intelligence in our hearing aids, 2023. Disponível em: <https://www.widexpro.com/en/widex-technology/artificial-intelligence/>. Acesso em: 26 de abril de 2023.

WORLD ECONOMIC FORUM. Artificial Intelligence for Children. 2022. Disponível em: https://www3.weforum.org/docs/WEF_Artificial_Intelligence_for_Children_2022.pdf. Acesso em: 10 de dezembro de 2022.

8. O DESAFIO DA REGULAÇÃO DA INTELIGÊNCIA ARTIFICIAL NA SAÚDE: ASPECTOS TÉCNICO-JURÍDICOS DA SEGURANÇA DAS INFORMAÇÕES

*THE CHALLENGE OF REGULATION OF ARTIFICIAL INTELLIGENCE IN HEALTH:
TECHNICAL-LEGAL ASPECTS OF INFORMATION SECURITY*



<https://doi.org/10.36592/9786554600552-08>

Maria Eugênia Londero Deggeroni¹

RESUMO

O artigo aborda as limitações da regulação da inteligência artificial na saúde, frente as medidas de cibersegurança, com o questionamento: observando o padrão específico e o ordenamento jurídico brasileiro, quais as medidas técnicas a serem tomadas no âmbito da inteligência artificial na saúde? O objetivo geral é estabelecer meios de proteção para que a inteligência artificial não seja uma fragilidade, ainda mais no caso dos dados de saúde. As metodologias são: dedutiva para a abordagem, comparativa para o procedimento, sistemática para a interpretação, sendo uma pesquisa teórico-bibliográfica, bem como documental. Os tópicos abordam sobre a inteligência artificial e sobre seu uso na saúde, bem como sobre a questão da cibersegurança e da proteção de dados, quanto aos desafios das ações maliciosas e ao Projeto de Lei selecionado, considerando as bibliografias. Conclui-se que é necessário que se compreenda a inteligência artificial e que as medidas técnicas sejam tomadas para evitar brechas que causem danos.

Palavras-chave: Cibersegurança. Medidas de segurança. Direito Fundamental à Dados Pessoais. Dados Pessoais Sensíveis. 5. Moldura regulatória.

¹ Doutoranda, Mestra e Bacharela em Direito pela Pontifícia Universidade Católica do Rio Grande do Sul. Especialista em Ciências Humanas: Sociologia, História e Filosofia pela PUCRS Online. cursando Especialização em Segurança da Informação na UNYLEYA (EAD). Advogada. Link Lattes: <http://lattes.cnpq.br/2092691360281397>. E-mail: maria.londero@edu.pucrs.br.

ABSTRACT

This article approaches the limitation of the regulation of artificial intelligence in health, in face of cybersecurity measures, with the question: observing the specific standards and Brazilian legal system, what are the technical measures in the scope of artificial intelligence in health? The general objective is to establish means of protection so artificial intelligence is not a fragility, even more on the case of health data. The methodologies are: deductive to approach, comparative to procedure, systematic to interpretation, being a theoretical and bibliographic research, as well as documentative. The topics address artificial intelligence and its use in health, as well as the issue of cybersecurity and data protection, the challenges of malicious actions and the selected bill, considering the bibliographies. It is concluded that it is necessary to understand artificial intelligence and that technical measures are taken to avoid breaches that cause damages.

Keywords: Cibersecurity. Security measures. Personal data fundamental right. Sensible data. Regulatory framework.

INTRODUÇÃO

A regulação da inteligência artificial na saúde deve visar medidas técnicas de segurança tecnológica, para garantir a proteção de dados pessoais, embora não seja abordada, com a ética ou a responsabilidade, estando estabelecido o recorte. A relevância é social (pelo impacto na sociedade), de atualidade (uso da inteligência artificial no âmbito da saúde e o cenário jurídico) e de reflexão (unindo os mais diferentes trabalhos, a fim de observar as medidas necessárias). A justificativa de estudo, portanto, é social, acadêmica (ampliar os estudos) e doutrinária-jurídica (ampliar as bases para os estudos futuros). O problema é: observando os padrões específicos e o ordenamento jurídico brasileiro, quais as medidas técnicas (cibersegurança) no âmbito da inteligência artificial na saúde? A hipótese é de que as medidas de criptografia e outras ferramentas podem auxiliar a proteger a inteligência artificial de agentes externos.

O objetivo geral é estabelecer as medidas para a segurança tecnológica na inteligência artificial no âmbito da saúde. Os objetivos específicos são: explicar a

inteligência artificial no âmbito da saúde, com exemplos; abordar a regulação da inteligência artificial; delimitar a base da segurança tecnológica e a relacionar à inteligência artificial; elencar os aspectos de segurança tecnológica na inteligência artificial na saúde e elaborar medidas técnicas básicas para concretizar esses aspectos, com base nas legislações e padrões, como já observado. O método de abordagem é dedutivo, a fim de abordar aos poucos os temas e desenvolver logicamente a análise. O método de procedimento é comparativo para estabelecer semelhanças e diferenças nos aspectos analisados. O método de interpretação é sistemático, buscando analisar considerações normativas e basear-se nelas para o estabelecimento das medidas.

A pesquisa é bibliográfica e documental, com uso de artigos, livros e outros materiais do primeiro grupo (com busca por palavras-chave no Google e no site da Biblioteca), padrões, legislações e guias, como os da Organização Mundial da Saúde. Será explicativa, a fim de analisar como as medidas podem auxiliar no cenário futuro e não apenas descrevê-las. Os tópicos são divididos em dois, o primeiro aborda a inteligência artificial no âmbito da saúde, contando com exemplos e considerando os aspectos jurídicos, com a base necessária para abordar a cibersegurança e a proteção de dados no seguinte, este que conta com os aspectos da injeção de códigos, perpassando elementos de segurança, vinculações dos padrões de saúde, a análise do Projeto Lei nº 21/20 e reflexões finais sobre a regulação.

1. A INTELIGÊNCIA ARTIFICIAL NO ÂMBITO DA SAÚDE: ANÁLISE DE EXEMPLOS E OS ASPECTOS JURÍDICOS INTRODUTÓRIOS

No primeiro tópico, será abordado o conceito, as delimitações didáticas, as divisões sobre o nível de aprendizado e sobre o tipo de verificação, a legislação sobre a inovação, dois atos normativos, a busca pelo conhecimento das tecnologias para realizar o estudo para uma regulação de alto nível, que represente o que há e não o faça por medo, sem compreender o objeto, visando o uso da saúde. No segundo ponto, será analisado sobre os exemplos e as verificações de autores sobre a saúde, visando compreender as bases de constitucionalidade e eficácia de direitos fundamentais, como a proteção de dados sensíveis, como os de saúde.

1.1 DO CONCEITO ÀS BASES DA INTELIGÊNCIA ARTIFICIAL: O USO EM QUESTÕES QUE ENVOLVEM DADOS DE SAÚDE

A análise de modelos de inteligência artificial avalia o funcionamento e a forma deste, mas não explica o que ocorre. Silva (2019, p. 41, 43) auxilia nessa questão demonstrando que há uma relação com a matemática e a estatística, em modo de funcionamento se daria como um modelo matemático-estatístico, pelo processamento de dados. A inteligência artificial foi estudada pelos mais diferentes autores (MCCARTHY, 2007, p. 2-5, 12-13; MITCHELL, 1997, p. 14-15, 21-36; TURING, A., 1950, p. 2, 10-12, 17-22; TURING, D., 2019, p. 86-103, 126, 170-193; WINSTON, 1993, p. 5-43). As verificações (MCCARTHY, 2007, p. 2-5, 12-13; TURING, A. 1950, p. 2, 10-12, 17-22) são parte das bases da inteligência artificial na medida em que as demais são ampliações dos estudos clássicos, auxiliando a pensar sobre as potencialidades.

Dermot Turing (2019, p. 86-103) avalia os usos e as abordagens atuais, com as mudanças desde que Alan criou o Teste – muito foi aprofundado e melhorado. Mitchell (1997, p. 14-15, 21-36) e Winston (1993, p. 5-43) auxiliam a compreender essas bases de aprofundamento. A construção se dá com base em “algoritmos” (AHO; HOPCROFT; ULIMAN, 1974, p. 8-52; SALVETTI, 1998, p. 10-24), que são arquitetados cada vez mais conforme as necessidades das organizações, com o desenvolvimento para processar os dados inseridos no modelo (IBMCLOUDEDUCATION, 2020c), porém, para que haja o melhor processamento possível, deve levar em conta as características. A inteligência artificial (IBMCLOUDEDUCATION, 2020a) pode ser dividida em “aprendizado de máquina” (IBMCLOUDEDUCATION, 2020c), “rede neural” (IBMCLOUDEDUCATION, 2020d) e “aprendizado profundo” (IBMCLOUDEDUCATION, 2020b), com a ampliação em nível de complexidade e autonomia, frente ao desenho dos modelos.

O aprendizado se dá com a processamento de dados, sendo um mecanismo de ajuste que amplia e especifica, conforme o próprio modelo (IBMCLOUDEDUCATION, 2020c). A rede é uma estrutura intermediária, com menores camadas e complexidade (IBMCLOUDEDUCATION, 2020d) e o aprendizado profundo amplia essas camadas e incorpora dados, atuando de forma mais “independente” e

menos “estruturada”, do qual a “CNN” é exemplo (IBMCLOUDEDUCATION, 2020b). Diferencia-se a fim de demonstrar que a “rede neural” é utilizada para desenvolver o “aprendizado profundo”, porém, que este é mais qualificado.

Há uma diferença sensível, a ponto de poder ser tratada como três níveis, com a compreensão de cada modelo, que deve ser orientado pelos dados que nele serão inseridos e pelas necessidades. Pode ser dividida em: “supervisionada” (IBMCLOUDEDUCATION, 2020c), na qual existe certo direcionamento de processamento de dados para uma saída, “semi-supervisionada” (ALBALATE; WOLFGANG, 2011, p. 15-25), que alarga a operação da supervisionada, com certa liberdade com o processamento dos dados, e “não supervisionada” (NILSSON, 1998, p. 119-130), que na qual o próprio modelo gera resultado sem preestabelecimentos, diferenciando-se pela interferência humana e pela construção do modelo – neste ponto, residindo uma diferenciação um pouco mais ampliada².

Observa-se na legislação, a Lei nº 10.973 (BRASIL, 2004) e o Decreto que a regulamenta (BRASIL, 2018a), o “incentivo à inovação [...]”, sendo que é necessário que, pela Lei citada, “[...] result[em] em melhorias e em efetivo ganho de qualidade ou desempenho [...]”³. No âmbito jurídico, o olhar para o tema deve ser vinculado com os impactos, não com a explicação ou previsão de conceitos, ou como (NOGUEIRA, 2022) observa, de legislações sem conhecer a fundo como a tecnologia funciona e, neste ponto, se concorda, parcialmente, com a observação das empresas de tecnologia sobre a legislação que vem sendo discutida na União Europeia (HEIKKILÄ, 2022)⁴. Há a necessidade de pensar e de realmente conhecer as tecnologias com base na realidade, excluindo as projeções ou compreensões incorretas sobre as tecnologias (NOGUEIRA, 2022), sendo um impeditivo para a realização de uma boa regulação por não abordar devidamente os impactos desta.

² A observação se dá por meio da noção de que, para alguns casos, dependendo da sensibilidade do tema ou dos dados, pode ser importante que haja uma maior participação humana.

³ Porém, é importante observar os limites constitucionais que auxiliam na extensão da “inovação”, esta prevista nos artigos 218 e 219 (BRASIL, 1988), na medida em que visa “a solução dos problemas brasileiros”, por exemplo, incluindo a necessidade de participação “interna” nessa troca.

⁴ Tal tema não é o principal deste estudo, porém essa base é importante para pensar na regulação da segurança das informações e, por fim, da proteção de dados processados por inteligência artificial.

Considerando a inteligência artificial no âmbito da saúde⁵ serão analisadas as realizações e as tecnologias existentes está dentro de um panorama que vem crescendo (ALAMI, 2020; ALBUQUERQUE, 2022; ANAHP, 2022; DAVENPORT, 2019, p. 94-98; FERREIRA JÚNIOR; CORREIA; MARQUES, 2019, p. 38-46; FATHIMA; SAMUEL, 2021, p. 144-152; LAWRY, 2020, 27-40; PATTNAYAK; JENA, 2021; VEDOVATE, 2021, p. 4-11) e que deve ser cuidado quanto ao aspecto da segurança lógica (CISCO, [s.d]). A atualização, no sentido de melhoria, é mecanismo basilar da cibersegurança e, com a relevância dos dados de saúde, estes sensíveis, torna-se necessário a ampliação de ferramentas e de cuidados para evitar que os riscos se tornem impacto, como será visto no segundo tópico.

Aliás, dentre as avaliações dos autores acima mencionados, Fathima e Samuel (2021, p. 144-152) se destacam, na medida em que é observado o que se denomina de “hiperparâmetro”, que também é observado por outros autores (PINA; NEVES; PAES, et al, 2019, p. 223-228), e a abordagem de questões relacionadas à exames e saúde, que se vincula diretamente com o caso. E é possível abordar os casos em que o tipo de aprendizado de máquina pode levar a crer que o melhor modelo seja o supervisionado, vinculado aos próprios hiperparâmetros mencionados acima, para manter certo controle e revisar os resultados, porém, tal estudo não é o objeto no momento e ficará para outro momento. Frente aos desafios atuais de integrar as tecnologias com as limitações já impostas pelos direitos fundamentais presentes no ordenamento ou que precisarão ser realizadas, tal como o que é previsto pela LGPD, artigo 46, parágrafo 1º (BRASIL, 2018).

Embora sejam relevantes para o auxílio, deve ser cuidada a forma de tratamento dos dados de saúde e se todos são necessários, frente ao que está sendo especificado na arquitetura do sistema, alguns dados podem ser apagados e o sistema ainda funciona da forma que foi projetado, resta ver, no caso concreto, quais seriam. Assim, evitam-se riscos desnecessários e restrições ainda maiores frente à capacitação e melhoria de cibersegurança, na medida em que diminui o impacto e o risco. O próximo subtópico visa observar exemplos do que há em matéria de uso na

⁵ O próprio personagem Baymax (OPERAÇÃO BIG HERO, 2014) é baseado na compreensão do impacto da inteligência artificial na saúde, mas também traz questionamentos sobre a interação homem-máquina e, juridicamente, sobre a proteção de dados – esse último é o aspecto jurídico principal.

saúde, a fim de tecer alguns comentários e auxiliar na considerações sobre as necessidades e limitações da regulação sobre o ponto específico.

1.2 OS EXEMPLOS DE USO DA INTELIGÊNCIA ARTIFICIAL NA SAÚDE: CONSIDERAÇÕES TECNOLÓGICO-JURÍDICAS

Como observado anteriormente, a ideia é revelar alguns exemplos sobre o uso e realizar alguns apontamentos, a fim de tornar mais concreto o estudo. Os exemplos citáveis são: "câncer" (ABRALE, 2017; HUNTER; HINDOCHA; LEE, 2022; KIROS, 2022), "covid" (MARQUES; FERREIRA; VERAS, et al, 2022, p. 148-156, 157-158, 170-177), exames de "raio x" (TIU; TALIU; PATEL, et al, 2022), de "olhos" (WANG, M., 2020), de coração (CORREIA, LOPES; PORTO; et al, 2021, p. 1063-1064, 1066, 1069; WEGNER, 2022; SILVA FILHO; COUTINHO, 2022, p. 4-11)⁶. São relevantes para a compreensão do cenário e das possibilidades de impactos jurídico, com a verificação dos aspectos regulatórios, com a base de proteção de dados, mas, principalmente, com a cibersegurança, que garante o aspecto citado.

Imagens são colocadas no sistema e a forma de leitura dos exames é treinada para que, com o processamento das imagens dos pacientes seja corretamente dimensionado. O reconhecimento de padrões resultante da inteligência artificial auxilia o médico no diagnóstico, porém, com base nos elementos elencados até o momento, é importante destacar a relevância do acompanhamento e revisão dos médicos para evitar erros e corrigir as balizas de treinamento, por exemplo, evitando danos aos indivíduos. Há a relação do direito digital (PINHEIRO, 2021, p. 71-126, 222-238, 329-334) e a concretização em constitucionalidade (SARLET, 2018, p. 265-282, 405-423; SARLET, 2022, 166-191, 490-499, 679-754), bem como a necessidade de repensar a inteligência artificial, quanto à eficácia da proteção de dados – de saúde,

⁶ Um dos cuidados é para que não ocorra como o exemplo, que separou pacientes por "raça" (GICHOYA, BANERJEE; BHIMIREDDY, et al., 2022), embora não seja o tema específico, a ideia é abordar esse cuidado. O destaque se faz tendo em vista que a informação não foi adivinhada pelo sistema, dados foram acrescentados, o que fez com que o processamento levasse em conta os mesmos, sendo que poderia não ser necessário para o tratamento e diagnóstico. Talvez essa seja uma premissa relevante a ser considerada pelos autores que estudam o tema na computação e engenharia de software, por exemplo.

tendo em vista os desafios para a segurança da informação, devendo a regulação se preocupar com os aspectos já mencionados.

Assim, o direito digital, frente as mudanças sociais, deve ter em vista à eficácia da proteção de dados, ainda mais em se tratando de dados sensíveis. São necessários limites decorrentes da própria necessidade da organização, esta que deve se comprometer com a concretização do direito fundamental. A inteligência artificial não é um desafio por si mesma, mas os desenvolvedores e quem insere os dados tem que ter noção do que é necessário para o funcionamento e deve conhecer o ciclo das informações, assim sendo necessária a interligação entre estes e os utilizadores do sistema criado. A meta, diante da reflexão sobre os apontamentos realizados até o momento, é o desenvolvimentos de sistemas seguros em relação à cibersegurança e à aspectos vinculados à direitos fundamentais.

A inteligência artificial descrita no âmbito jurídico (TEIXEIRA; CHELIGA, 2019, p. 13-18, 22, 87-101; SOUZA; OLIVEIRA, 2019, p. 65-81; STEIBEL; VICENTE; JESUS, 2019, p. 53-64) se diferencia da abordagem técnica já citada, na medida em que o segundo grupo observa os cálculos relacionados à inteligência artificial, sendo um exemplo Fathima e Samuel (2021, p. 138-152) e o outro Silva (2019, p. 35-38, 41-45), portanto, fica-se com a descrição técnica já comentadas. A questão já foi abordada pela Organização Mundial da Saúde, com um guia, abordando as considerações mínimas quanto às necessidades para a implementação de tecnologias de inteligência artificial no âmbito da saúde (OMS, 2021, p. 6-22). Este pode ser utilizado para a análise das regulações propostas, podendo ser ampliado ou não conforme as necessidades e objetivos que o Brasil almeja.

Diante do que se observou até o momento a questão da constitucionalidade do uso da tecnologia está diretamente relacionada com a ótica do direito digital no âmbito da segurança em relação às informação de saúde, ou seja, não pode violar direitos fundamentais ou deve mitigar os efeitos causados. Há a necessidade de cuidados com a arquitetura, com a base no código e nas vulnerabilidades, a fim de que seja estabelecido um mínimo de segurança, com as delimitações de necessidades, e não ultrapassando o fato de que as organizações estabelecem como premissas de segurança. Assim, passa-se para o próximo tópico, abordando-se sobre a cibersegurança e as necessidades para a proteção dos indivíduos que tem

seus dados pessoais sensíveis tratados para cuidados de saúde, mesmo que saudáveis.

2. A CIBERSEGURANÇA E A PROTEÇÃO DE DADOS: AS MEDIDAS PARA MITIGAR DANOS E AS LIMITAÇÕES DA REGULAÇÃO

No primeiro ponto deste tópico, a busca é pelo recorte de cibersegurança, sendo necessário o cuidado com as bases da segurança da informação, com a observação da injeção de malwares, das nuvens e os problemas causados pela brechas, com o ideal de compreender a questão constitucional, com aspectos que serão ampliados no segundo ponto, que foram complicados com a pandemia, com o uso do acesso remoto. No segundo ponto, o foco é apresentar a regulação em si, porém, com a base já verificada. A legislação será observada com a doutrina, com a consideração do direito fundamental, do artigo 5º da Constituição Federal quanto à proteção de dados, com um Projeto de Lei nº 21/20, com a verificação da inteligência artificial e das possibilidades de reinterpretação com a atualização da leitura dos artigos constitucionais, a fim de ampliar a visão.

2.1 A SEGURANÇA DA INFORMAÇÃO LÓGICA E A MITIGAÇÃO DOS RISCOS: DA PROTEÇÃO DO INDIVÍDUO FRENTE AOS POSSÍVEIS DANOS

Os aspectos de segurança tecnológica, ou cibersegurança (MICROSOFT, [s.d]) na inteligência artificial na saúde devem ser cuidados ainda mais na medida em que pode haver injeção de “códigos maliciosos” em “redes neurais” (WANG; LIU; CUI, 2021, p. 1-7). A base da segurança tecnológica quanto à inteligência artificial deve levar em conta as nuvens (ORACLE, [s.d]) e os problemas que devem ser gerenciados (ANDRIETTA; GEUS, 2021, p. 8-10, 14-21; OWASP, [s.d], p. 7-10; MASSIMI, 2021; ZANUTTO, [s.d], p. 1-6) e com base no padrão já existente (LEARNMICROSOFT, 2021), porém, com as atualizações que surgirem.

Ou seja, os mecanismos de guarda de servidores, por exemplo, que não necessitam mais ser físicos, sendo um conjuntos de recursos que pode armazenar todo o tipo de dados, com alguns desafios a serem resolvidos ainda, com a escolha

do modelo necessário para a organização, da segurança visada, com base nos dados armazenados e na escalabilidade, o que causaria potencial risco às informações sensíveis contidas nos bancos de dados. Não está sendo realizado um diagnóstico preciso, mas está sendo observado que deve ser cuidado, conforme as premissas sobre os dados e a legislação concernente, por exemplo, os pessoais têm verificado na Lei Geral de Proteção de Dados (BRASIL, 2018), mas que seguem as boas práticas – um conjunto delimitado e não determinado de mecanismos que visam a garantia de segurança, conforme a necessidade organizacional e dos dados.

A segurança da informação (CISCO, [s.d]; MASCARENHAS NETO; ARAÚJO, 2019, p. 17-74, 142-147; MITTECHNOLOGYREVIEWINSIGHTS, 2022) deve ser vista como meio de observar fins constitucionais (BRASIL, 1988), utilizando mecanismos de inteligência artificial para construir a segurança (KAMHOUA; KIERKINTVELD; FANF, et al, 2021, p. 10-26), principalmente no âmbito da saúde (MUYLDER; OLIVEIRA; BATISTA, 2019, p. 222-223, 225-226, 228-229), no qual há os padrões de segurança e de saúde (NGQONDI, 2009, p. 31-41, 52-66; ORLETTI, 2021; SEGOVIA, 2016). A questão aqui é a proteção do indivíduo perante os danos, privacidade, proteção dos dados, dentre outros problemas possíveis que são amplamente conhecidos no cenário jurídico.

Então, o que é proposto é o uso da inteligência artificial como plataforma de auxílio de diagnóstico, porém, com o uso desta para auxiliar na cibersegurança, com as mais diferentes ferramentas conhecidas e que sejam necessárias no contexto, tendo em vista a relevância dos dados, como abordado nos materiais já mencionados e nos padrões, destacando-se o observado por Ngqondi (2009, p. 31-41, 52-66). O motivo de citar a nuvem⁷ é que, além de seus usos possíveis como os citados, foi utilizado na época da COVID-19 (SAÚDEBUSINESS, 2021) e é importante notar que a União Europeia elaborou guia para auxiliar diretamente na “proteção de dados” (UNIÃO EUROPEIA, 2020), no qual foi previsto sobre a segurança dos

⁷A “nuvem” pode ser compreendida como uma replicação do cenário físico de “infraestrutura”, porém, com o acesso “via *internet*”, com a ótica de diversos tipos, que operam de forma diversa, com o fim almejado pela organização, que pode querer “opções pré-prontas”, como a “SaaS” (ANDRIETTA, GEUS, 2021). Sobre o uso de nuvem, tem-se Andrietta e Geus (2021), Learnmicrosoft (2021), Massimi (2021), o exemplo da Oracle especificamente para a saúde (ORACLE, [s.d]) e a análise do OWASP ([s.d]), que auxilia muito a pensar sobre a segurança em diversas abordagens.

“aplicativos” que foram usados nesse período. Demonstrou-se a preocupação, tendo em vista que a verificação de aumento de acesso remoto na e pós-pandemia. Passa-se para a análise regulatória, em si, quanto a consideração da abordagem da cibersegurança como garantia para o bom funcionamento.

2.2 DA REGULAÇÃO DA INTELIGÊNCIA ARTIFICIAL: A PROTEÇÃO DE DADOS COMO PONTO DE PARTIDA DA PREVISÃO

A ideia estudada, dentre as demais, é a melhor, na medida em que representa de forma menos projetada a tecnologia. Tendo em vista as propostas no Projeto e visando contribuir, há alguns aspectos que devem ser previstos de outra forma. A regulação da inteligência artificial, segue a base da Lei Geral de Proteção de Dados (BRASIL, 2018b), que trata os dados de saúde como “sensíveis”, com base nos aspectos doutrinários da proteção de dados (DONEDA, 2021, p. 143-146; NASCIMENTO; MARQUES; COSTA, 2020, p. 209-211, 214-216, 224-226; POETA, 2020, p. 80-104; TEIXEIRA; ARMELIN, 2021, p. 136-145), foi possível vincular com a questão específica da saúde e a regulação (ASSESSPRORS, [s.d]; ALMEIDA, 2022, p. 28-31; BRAGANÇA, 2022, p. 19-22; OLIVEIRA; VEIGA; COZMAN, 2022, p. 28-31), tendo em vista a previsão de direito fundamental de proteção de dados (BRASIL, 1988) e os problemas possíveis de segurança (TUBINO, 2022).

Dentre as regulações propostas, diante do que foi abordado até o momento, a que se destaca frente às demais é a proposta por Eduardo Bismarck, Projeto de Lei nº 21, de 2020 (BRASIL, 2020), pois parece ser, dentro dos três projetos (os demais não serão observados em razão do espaço), o mais próximo de um ideal legislativo, embora ainda necessite de diálogo e avaliação para a melhoria, nos artigos 2º (conceito de “inteligência artificial”), *caput* e incisos, o artigo 3º (“objetivo”, que traz uma necessidade de ampliar as observações), o artigo 4º e seus incisos (a fim de avaliar os “fundamentos”, com a previsão da “segurança” no inciso VIII e IX, sendo que o que será abordado é o segundo, pois, como já foi observado a base é da segurança da informação e seus aspectos legais e não a proteção de dados em si), o artigo 5º (dos “princípios”, dos quais prevê-se a “segurança e prevenção”, no inciso VI, devendo ser ampliado) e ao artigo 6º, parágrafo 2º, sendo que os demais pontos

não serão abordados na medida em que não se vinculam com a relação da segurança tecnológica (BRASIL, 2020). A partir disso, passa-se para os resultados.

Não há a verificação de aspectos de segurança sendo ainda mais genéricas do que a Lei Geral de Proteção de Dados (BRASIL, 2018) e ignorando a possibilidade de uso da inteligência artificial para a cibersegurança e, assim sendo, proteção de dados, pois seria importante retratar essa base, tal como a verificação de delimitações ao modelo, diante da necessidade dos dados, por exemplo. O exemplo de código injetado, como comentado, no âmbito de uma rede neural tem relação direta com a segurança de informação e com a proteção de dados, sendo que ela deve ter um nível aceitável tanto no âmbito de controle quanto no âmbito que vem crescendo (a nuvem), que ainda não construiu bases tão seguras, sendo necessária a atualização e a melhoria contínua. Na medida em que os exemplos se vinculam à dados sensíveis, cuidados são necessários para evitar o impacto aos indivíduos, como já comentado.

Assim, é relevante considerar a adequação do projeto citado para pensar sobre tais pontos, para revisar e ampliar para se aproximar das bases da segurança da informação, por certo considerando a necessidade de respeitar os limites dos padrões ante as necessidades das organizações, o que de certa forma também já foi observado na Lei Geral de Proteção de Dados (BRASIL, 2018). Dentre os resultados, com a conjugação dos pontos, foi pensado na possibilidade do direitos fundamental à segurança da informação, já que é inerente à proteção de dados como garantidor desta. Parece ser um contexto importante no âmbito da sociedade da informação, pensando o artigo 5º, inciso e o artigo 6º, caput da Constituição Federal (BRASIL, 1988), porém, este tema necessita de maiores aprofundamentos, restando como uma abordagem a ser pesquisada no futuro.

Pode ser necessário, ainda, o estudo de desenvolvimento de padrões sobre a inteligência artificial e estes deverão ser levados em conta para a observação regulatória, devendo estas serem atualizadas para atuarem na limitação que os *standards* permitem, levando em conta o que Nogueira (2022) observou: se não há o profundo conhecimento técnico, há a falta das premissas necessárias e o problema da diminuição da inovação, já consideradas na Constituição e em Decreto. O projeto que foi elaborado precisará ser revisto por técnicos para que reflita a realidade antes

que qualquer movimentação seja realizada, caso contrário, "já estará de certa forma ultrapassada" (FRANCO, 2023). A questão é que não é apenas o desenvolvimento tecnológico (FRANCO, 2023), este que também aparece na Constituição, em seu artigo 218 (BRASIL, 1988). Dois aspectos são destacados na abordagem, a previsão da aplicação da inteligência artificial e a observação da "transparência" e da "explicabilidade" como fatores relevantes (FRANCO, 2023).

Observa-se, então, que a questão não é o desenvolvimento e a liberdade das empresas como Franco (2023) considera, os problemas são mais graves: as soluções que podem auxiliar nos diagnósticos sendo limitadas, a amplitude de softwares regulados pode ser um empecilho, o conjunto de amostra dos modelos deve ser equilibrado para evitar erros evitáveis, o acúmulo de dados que provavelmente não seriam necessários e que podem ser violados sem o cuidado com os bancos de dados, a segurança, diante do que é proposto leitura de atualização do artigo 6º da Constituição Federal (BRASIL, 1988), a ser ampliada para o contexto digital. Notou-se que a responsabilidade elencada por Franco (2023) quanto aos "usos indevidos" não é suficiente, ao menos com tal terminologia, com o próprio exemplo da cibersegurança que foi analisada neste artigo, mas ainda há que se explorar sobre esse ponto, porém, em outros estudos. A partir de tais considerações, parte-se para a conclusão, a fim de dar um fechamento para os elementos estudados neste artigo.

CONCLUSÕES

Foi observado que as medidas técnicas necessárias, já se considerando a base constitucional-digital na segurança da informação, a observação de direito fundamental – a ser ampliada no artigo e a legislação, são a abordagem da arquitetura em si, no código em si, com a necessidade de cuidado nas brechas possíveis, e as noções de vulnerabilidades em geral – considerando a avaliação prevista na ISO (o padrão), principalmente considerando a noção da importância da informação relacionada à saúde, e considerando o aumento do número de uso da nuvem no caso. No cenário estudado, com as pesquisas realizadas e no tempo disponível de desenvolvimento foram essas as considerações possíveis.

A busca é desenvolver mais os estudos, a partir dos pontos já delimitados nos demais elementos deste resumo, tentando extrair mais inferências para, enfim, solucionar mais amplamente o problema proposto. Observa-se, então, a necessidade de revisão de códigos e de proteções para evitar alterações maliciosas; adaptar os padrões às necessidades das organizações, adequando a arquitetura frente aos dados que estão sob seu controle; atualizar as políticas, com base em alterações nos padrões pelas entidades responsáveis; manter armazenamentos para auditorias, o cuidado com os bancos de dados e com a forma da inteligência artificial, frente às necessidades, evitando dados que não auxiliam na solução, bem como o uso da mesma para auxiliar na segurança dos dados. Assim, observa-se que o problema foi respondido, os objetivos foram cumpridos, ao menos frente ao recorte, porém, ainda há muito a ser pesquisado sobre o tema.

REFERÊNCIAS

ABRALE. **Clínica utiliza inteligência artificial contra o câncer**. 10 jul. 2017. Disponível em: <https://www.abrale.org.br/noticias/clinica-utiliza-inteligencia-artificial-contra-o-cancer/>. Acesso em: 25 out. 2022.

AHO, Alfred V; HOPCROFT, John E; ULIMAN, Jeffreu D. **The design and analysis of computer algorithms**. Massachusetts, California, London, Amsterdam, Ontario, etc: Addison-Wesley Publishing Company, 1974.

ALAMI, Hassane; LEHOUX, Pascale; AUCLAIR, Yannick; et al. **Artificial Intelligence and Health Technology Assessment: Anticipating a New Level of Complexity**. J Med Internet Res, 22, 7, e17707, [s.p], jul 2020. Disponível em: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7380986/>. Acesso em: 13 out. 2022.

ALBALATE, Amparo; WOLGANG, Minker. **Semi-supervised and unsupervised machine learning: novel strategies**. London, Hoboken, New Jersey: ISTE, Wiley, 2011. Acesso online via Biblioteca PUCRS.

ALBUQUERQUE, Manoela. Big Data, IA e canais digitais a favor da saúde corporativa. **MIT Technology Review**, 30 set. 2022. Disponível em: <https://mittechreview.com.br/big-data-ia-e-canais-digitais-a-favor-da-saude-corporativa/>. Acesso em: 13 out. 2022.

ALMEIDA, Patricia Gomes Rêgo de. Regulação da Inteligência Artificial: ação coletiva que requer governança? **Computação Brasil** – Revista da Sociedade

Brasileira de Computação, n. 47, p. 28-31, jul. 2022. In: https://www.sbc.org.br/images/flippingbook/computacaobrasil/computa_47/pdf/CompBrasil_47.pdf. Acesso em: 13 out. 2022.

ANAHP. **Inteligência Artificial enfrenta o desafio de mostrar valor ao setor de saúde**. 25 fev. 2022. [s.l.] Disponível em: <https://www.anahp.com.br/noticias/noticias-anahp/inteligencia-artificial-enfrenta-o-desafio-de-mostrar-valor-ao-setor-de-saude/>. Acesso em: 13 out. 2022.

ANDRIETTA, Murilo Guidetti; GEUS, Paulo Lício de. **Categorização dos Desafios de Segurança em Nuvem relacionados à tecnologia de Virtualização**. Relatório Técnico IC-PFG-21-52. Projeto Final de Graduação. Dez. 2021. Disponível em: <https://www.ic.unicamp.br/~reltech/PFG/2021/PFG-21-52.pdf>. Acesso em: 13 out. 2022.

ASSESPRORS. **Os impactos da LGPD na saúde e a inclusão da IA nos processos**. [s.d] Porto Alegre. Disponível em: <https://www.assespro-rs.org.br/os-impactos-da-lgpd-na-saude-e-a-inclusao-da-ia-nos-processos/>. Acesso em: 13 out. 2022.

BRAGANÇA, Fernanda; BRAGA, Renata. Os desafios da regulamentação da Inteligência Artificial no Brasil. **Computação Brasil** – Revista da Sociedade Brasileira de Computação, n. 47, p. 19-22, jul. 2022. In: https://www.sbc.org.br/images/flippingbook/computacaobrasil/computa_47/pdf/CompBrasil_47.pdf. Acesso em: 13 out. 2022.

BRASIL. [Constituição (1988)] **Constituição da República Federativa do Brasil de 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 13 out. 2022.

BRASIL. **Decreto nº 9.283, de 7 de fevereiro de 2018**. Regulamenta a Lei nº 10.973, de 2 de dezembro de 2004 [...]. 2018a. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/d9283.htm. Acesso em: 13 out. 2022.

BRASIL. **Lei nº 10.973, de 2 de dezembro de 2004**. Dispõe sobre incentivos à inovação e à pesquisa científica e tecnológica no ambiente produtivo e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2004/lei/l10.973.htm. Acesso em: 13 out. 2022.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). 2018b. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 13 out. 2022.

BRASIL. Senado Federal. **Projeto de Lei nº 21, de 2020**. Autoria: Deputado Federal Eduardo Bismarck (PDT/CE). Disponível em: <https://legis.senado.leg.br/sdleg->

getter/documento?dm=8939920&ts=1656530049593&disposition=inline. Acesso em: 13 out. 2022.

CHELIGA, Vinicius; TEIXEIRA, Tarcísio. **Inteligência Artificial: aspectos jurídicos**. Salvador: Juspodivm, 2019. 112 p.

CISCO. **O que é segurança da TI?** [s.d] Disponível em: https://www.cisco.com/c/pt_br/products/security/what-is-it-security.html. Acesso em: 13 out. 2022.

CORREIA, Luis; LOPES, Daniel; PORTO, João Vitor, et al. Validação de um algoritmo de inteligência artificial para a predição diagnóstica de doença coronariana: comparação com um modelo estatístico tradicional. **Arq. Bras. Cardiol – Sociedade Brasileira de Cardiologia**. v. 117, n. 6, p. 1061-1070, 2021. Disponível em: <https://www.scielo.br/j/abc/a/zGPqb6LYhvFy7W3dLJJcggP/?format=pdf&lang=pt>. Acesso em: 08 set. 2022.

DAVENPORT, Thomas; KALAKOTA, Ravi. The potential for artificial intelligence in healthcare. **Future Health J**, 6, 2, p. 94-98, jun. 2019. Disponível em: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6616181/>. Acesso em: 13 out. 2022.

DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados**. 3 ed. São Paulo: Thomson Reuters Brasil, 2021. 368 p.

FATHIMA, M. Dhilsath; SAMUEL, S. Justin. Hyperparameter Tuning of Ensemble Classifiers Using Grid Search and Random Search for Prediction of Heart Disease. p. 139-158. In: JENA, Om Prakash; TRIPATHY, Alok Ranjan; ELNGAR, Ahmed A.; et al. **Computational intelligence and healthcare informatics**. Hoboken, NJ; Beverly, MA: Wiley; Scrivener Publishing, 2021. Acesso online via Biblioteca PUCRS.

FERREIRA JÚNIOR, José Raniery; CORREIA, Natália Santana Chiari; MARQUES, Paulo Mazzoncini de Azevedo. Aprendizado de máquina na atenção à saúde humana. **Computação Brasil**, Revista da Sociedade Brasileira de Computação, v. 39, e. 1, p. 37-46, 2019. Disponível em: https://www.sbc.org.br/images/flippingbook/computacaobrasil/computa_39/pdf/CompBrasil_39_180.pdf. Acesso em: 13 out. 2022.

FRANCO, Rafael. **Por que uma Lei pode dificultar o desenvolvimento da inteligência artificial no Brasil**. Opinião CNN. 17 jan. 2023, às 06:00. Disponível em: <https://www.cnnbrasil.com.br/forum-opinioao/porque-uma-lei-pode-dificultar-o-desenvolvimento-da-inteligencia-artificial-no-brasil/>. Acesso em: 17 jan. 2023.

GICHOYA, Judy Wawira; BANERJEE, Imon; BHIMIREDDY, Ananth, et al. **AI recognition of patient race in medical imaging: a modelling study**. The Lancet Digital Health. 11 maio 2022. Disponível em:

[https://www.thelancet.com/journals/landig/article/PIIS2589-7500\(22\)00063-2/fulltext](https://www.thelancet.com/journals/landig/article/PIIS2589-7500(22)00063-2/fulltext). Acesso em: 13 out. 2022.

HEIKKILÄ, Melissa. **The EU wants to put companies on the hook for harmful AI**. 1 out. 2022. Disponível em: <https://www.technologyreview.com/2022/10/01/1060539/eu-tech-policy-harmful-ai-liability/>. Acesso em: <https://www.technologyreview.com/2022/10/01/1060539/eu-tech-policy-harmful-ai-liability/>. Acesso em: 13 out. 2022.

HUNTER, Benjamin; HINDOCHA, Summet; LEE, Richard W. The Role of Artificial Intelligence in Early Cancer Diagnosis. **MDPI Cancers**, 14, 6, [s.p], mar. 2022. Disponível em: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8946688/>. Acesso em: 13 out. 2022.

IBMCLOUDEDUCATION. **Artificial Intelligence (AI)**. 3 jun. 2020. 2020a. IBM Cloud Learn Hub. Disponível em: <https://www.ibm.com/cloud/learn/what-is-artificial-intelligence>. Acesso em: 13 out. 2022.

IBMCLOUDEDUCATION. **Deep Learning**. 1 maio 2020. 2020b. IBM Cloud Learn Hub. Disponível em: <https://www.ibm.com/cloud/learn/deep-learning>. Acesso em: 13 out. 2022.

IBMCLOUDEDUCATION. **Machine learning**. 15 jul. 2020. 2020c. IBM Cloud Learn Hub. Disponível em: <https://www.ibm.com/cloud/learn/machine-learning>. Acesso em: 13 out. 2022.

IBMCLOUDEDUCATION. **Neural Networks**. 17 ago. 2020. 2020d. IBM Cloud Learn Hub. Disponível em: <https://www.ibm.com/cloud/learn/neural-networks>. Acesso em: 13 out. 2022.

KAMHOUA, Charles A; KIERKINTVELD, Christopher D; FANF, Fei; et al. **Game theory and machine learning for cyber security**. Hoboken, New Jersey: John Wiley & Sons, 2021. Acesso online via Biblioteca PUCRS.

KIROS, Hana. **Doctors using AI catch breast cancer more often than does alone**. MIT Technology Review. 11 jul. 2022. Disponível em: <https://www.technologyreview.com/2022/07/11/1055677/ai-diagnose-breast-cancermammograms/#:~:text=A%20new%20study%20shows%20that,%2C%20dramatically%20reducing%20radiologists'%20workloads.&text=Radiologists%20assisted%20by%20an%20AI,alone%2C%20according%20to%20new%20research>. Acesso em: 13 out. 2022.

LAWRY, Tom. **AI in healthcare: a leader's guide to winning in the new age of intelligent health systems**. Boca Raton, Flórida: CRC Press, Taylor & Francis Group, 2020. Acesso online via Biblioteca PUCRS.

LEARNMICROSOFT. **Código de Conduta ISO/IEC 27018 para Proteção de Dados Pessoais na Nuvem**. 13 set. 2021. Colaboradores do artigo: robmazz; olprod. Learn Microsoft. Disponível em: <https://learn.microsoft.com/pt-br/compliance/regulatory/offering-iso-27018>. Acesso em: 13 out. 2022.

MARQUES, Júlio V. M.; FERREIRA, José F. C.; VERAS, Rodrigo M. S., et al. Classificação e segmentação de COVID-19 em imagens de tomografia computadorizada usando aprendizado profundo. p. 146-185. In: OLIVEIRA, Lucas Ferrari de; ARAÚJO, Flávio Henrique Duarte de. Livro de Minicursos – **SBCAS 2022: XXII Simpósio Brasileiro de Computação Aplicada à Saúde: 07 a 10 de junho de 2022**. Porto Alegre: Sociedade Brasileira de Computação, 2022. 269 p. Disponível em: <https://sol.sbc.org.br/livros/index.php/sbc/catalog/download/105/468/741-1?inline=1>. Acesso em: 13 out. 2022.

MASCARENHAS NETO, Pedro Tenório; ARAÚJO, Wagner Junqueira. **Segurança da informação: uma visão sistêmica para implantação em organizações**. João Pessoa: Editora da UFPB, 2019. 160 p. ePDF. Disponível em: <http://www.editora.ufpb.br/sistema/press5/index.php/UFPB/catalog/download/209/75/905-1?inline=1>. Acesso em: 13 out. 2022.

MASSIMI, Michael. **5 itens de segurança em nuvem indispensáveis para 2021**. 31 maio 2021. IBM Comunica. Disponível em: <https://www.ibm.com/blogs/ibm-comunica/5-itens-seguranca-em-nuvem/>. Acesso em: 13 out. 2022.

MCCARTHY, John. **What is artificial intelligence?** 12 nov. 2007. p. 1-15. Disponível em: <http://www-formal.stanford.edu/jmc/whatisai.pdf>. Acesso em: 13 out. 2022.

MEDEIROS, Claudia Bauzer. Dados, algoritmos, máquinas e pessoas. **Computação Brasil – Revista da Sociedade Brasileira de Computação**, n. 47, p. 11-14, jul. 2022. In: https://www.sbc.org.br/images/flippingbook/computacaobrasil/computa_47/pdf/CompBrasil_47.pdf. Acesso em: 13 out. 2022.

MICROSOFT. **O que é InfoSec (segurança da informação)?** Proteja as informações confidenciais em nuvens, aplicativos e outros pontos de extremidade. Perguntas frequentes: Qual a diferença entre segurança cibernética e segurança da informação. [s.d] Disponível em: <https://www.microsoft.com/pt-br/security/business/security-101/what-is-information-security-infosec>. Acesso em: 13 out. 2022.

MITCHELL, Tom M. **Machine Learning**. Boston: MCGRAW-Hill, 1997. 414 p.

MITTECHNOLOGYREVIEWINSIGHTS. **Cyber resilience melds data security and protection**. 12 out. 2022. Disponível em: <https://www.technologyreview.com/2022/10/12/1059904/cyber-resilience-melds-data-security-and-protection/>. Acesso em: 13 out. 2022.

MUYLDER, Cristiana Fernandes de; OLIVEIRA, Jeferson Gonçalves; BATISTA, Cássio Luís, et al. Segurança da informação e a área da saúde: a convergência dos temas e a intensidade das publicações científicas. **Revista de Gestão e Sistemas de Saúde**, São Paulo, v. 8, n. 2, p. 221-232, maio/ago. 2019. Disponível em: <https://periodicos.uninove.br/revistargss/article/view/14139/7683>. Acesso em: 13 out. 2022.

NASCIMENTO, João Carlos Hipólito Bernardes do; MARQUES, Maria Leonildes Boavista Gomes Castelo Branco; COSTA, Nayara Hanna Santiago, et al. **Inteligência artificial na Saúde e a proteção de dados**: reflexos da crise covid-19. *Direitos Fundamentais e Justiça*, Belo Horizonte, v. 14, n. 1, p. 207-230, nov. 2020. Disponível em: <https://dfj.emnuvens.com.br/dfj/article/view/964/1001>. Acesso em: 13 out. 2022.

NGQONDI, Tembisa. **The ISO/IEC 27002 and ISO/IEC 27799 Information Security Management Standards**: A Comparative Analysis from a Healthcare Perspective. Dissertação (Mestrado em Tecnologia da Informação), Faculdade de Engenharia, Ambiente Construído e Tecnologia da Informação, Nelson Mandela Metropolitan University, 2009. 133 p. Disponível em: <https://core.ac.uk/download/pdf/145049474.pdf>. Acesso em: 13 out. 2022.

NILSSON, Nils J. **Introduction to Machine Learning: an early draft of a proposed textbook**. 3 nov. 1998. Disponível em: <https://ai.stanford.edu/~nilsson/MLBOOK.pdf>. Acesso em: 13 out. 2022.

NOGUEIRA, Michele. **Risco Cibernético e a Arte na Cibersegurança**. 17 jun. 2022. Disponível em: <http://horizontes.sbc.org.br/index.php/2022/06/risco-cibernetico/>. Acesso em: 13 out. 2022.

OLIVEIRA, Cristina Godoy Bernardo de; VEIGA, João Paulo Cândia; COZMAN, Fabio G. Regulação da Inteligência Artificial: qual modelo adotar? **Computação Brasil** – Revista da Sociedade Brasileira de Computação, n. 47, p. 28-31, jul. 2022. In: https://www.sbc.org.br/images/flippingbook/computacaobrasil/computa_47/pdf/CompBrasil_47.pdf. Acesso em: 13 out. 2022.

OMS. **Ethics and Governance of Artificial Intelligence for Health**: WHO Guidance. Geneva: World Health Organization, 2021. Licence: CC BY-NC-SA 3.0 IGO. Disponível em: <https://www.who.int/publications/i/item/9789240029200>. Acesso em: 13 out. 2022.

OPERAÇÃO BIG HERO. Animação. Direção: Don Hall; Chris Williams. 2014. 1h42min.

ORACLE. **Oracle Cloud Infrastructure para Saúde**. [s.d] Disponível em: <https://www.oracle.com/br/industries/healthcare/cloud/>. Acesso em: 13 out. 2022.

ORLETTI, Danieli. **ISO 27799 e ISO 27001**: entenda a importância dessas normas na área da saúde. 18 ago. 2021. Neomed. Disponível em: <https://neomed.com.br/iso->

27799-e-iso-27001-entenda-a-importancia-dessas-normas-na-area-da-saude/. Acesso em: 13 out. 2022.

OWASP. **Segurança em Nuvem: a ameaça fantasma.** [s.d] Disponível em: <https://owasp.org/www-chapter-natal/assets/files/seguranca-em-nurvem.pdf>. Acesso em: 13 out. 2022.

PATTNAYAK, Parthasarathi; JENA, Om Prakash. Innovation on Machine Learning in Healthcare Services – An Introduction. p. 3-16. In: MOHANTY, Sachi Nandan. **Machine learning for healthcare application.** Hoboken, New Jersey; Beverly, Massachusetts: John Wiley & Sons, Scrivener Publishing, 2021. 389 p. Acesso online via Biblioteca PUCRS.

PINA, Débora B.; NEVES, Liliane; PAES, Aline; et al. **Análise de Hiperparâmetros de Aprendizado Profundo por meio de Dados de Proviência.** In: Anais do XXXIV Simpósio Brasileiro de Banco de Dados, Porto Alegre: Sociedade Brasileira de Computação, 2019. p. 223-228. Disponível em: <https://sol.sbc.org.br/index.php/sbbd/article/view/8827>. Acesso em: 30 jan. 2023.

PINHEIRO, Patrícia Peck. **Direito Digital.** 7 ed. rev. atual. e ampl. São Paulo: Saraiva Educação, 2021. 760 p.

POETA, Vitor Sardagna. **A inteligência artificial e a proteção de dados pessoais: reflexos do Regulamento Geral de Proteção de Dados Europeu (RGPD) no âmbito da garantia dos Direitos Fundamentais no Direito Brasileiro.** Dissertação (Mestrado em Ciência Jurídica), Programa de Pós-Graduação em Ciência Jurídica, Itajaí, 2020. Orientador. Alexandre Morais da Rosa. Disponível em: <https://www.univali.br/Lists/TrabalhosMestrado/Attachments/3015/DISSERTA%C3%87%C3%83O%20-%20VITOR%20SARDAGNA%20POETA.pdf>. Acesso em: 13 out. 2022.

SALVETTI, Dirceu Douglas. **Algoritmos.** São Paulo: Makron Books, 1998.

SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. **Curso de Direito Constitucional.** 11 ed. São Paulo: SaraivaJur, 2022. 1592 p.

SARLET, Ingo Wolfgang. **Eficácia dos Direitos Fundamentais: uma teoria geral dos direitos fundamentais na perspectiva constitucional.** 13 ed. ver. e atual. Porto Alegre: Livraria do Advogado, 2018. 515 p.

SAÚDEBUSINESS. **IA, IOT e nuvem possibilitam diagnóstico da COVID-19 em 30 minutos.** TI e Inovação. 17 maio 2021. Disponível em: <https://www.saudebusiness.com/ti-e-inovacao/ia-iot-e-nuvem-possibilitam-diagnostico-da-covid-19-em-ate-30-minutos>. Acesso em: 13 out. 2022.

SEGOVIA, Antonio José. **Como a ISO 27001 e a ISO 27799 se complementam em organizações de saúde.** 14 jun. 2016. 27001 Academy. Disponível em:

<https://advisera.com/27001academy/pt-br/blog/2016/06/14/como-a-iso-27001-e-a-iso-27799-se-complementam-em-organizacoes-de-saude/#:~:text=A%20principal%20similaridade%20entre%20ambas,%2C%20SoA%2C%20etc.>). Acesso em: 13 out. 2022.

SILVA, Gracemerce Camboim Jatobá e. Responsabilidade civil e a utilização de robôs de assistência à saúde e análise do diagnóstico com inteligência artificial no Brasil: quem deve ser responsabilizado em caso de dano à saúde? **Revista Jurídica da Seção Judiciária de Pernambuco**, v. 2, n. 13, 2021. Disponível em: <https://revista.jfpe.jus.br/index.php/RJSJPE/article/view/244>. Acesso em: 13 out. 2022.

SILVA, Nilton Correia da. Inteligência Artificial. p. 35-52. In: FRAZÃO, Ana; MULHOLLAND, Caitlin. **Inteligência Artificial: ética, regulação e responsabilidade**. São Paulo: Thomson Reuters, 2019.

SILVA FILHO, Francisco Ramos da; COUTINHO, Emanuel F. Aprendizado de Máquina para Predição de Diagnósticos de Doenças Cardiovasculares. p. 358-369. In: ITO, Márcio; SILVA, Romuere Rodrigues Veloso e (org.). **Anais do XXII Simpósio Brasileiro de Computação Aplicada à Saúde (SBCAS 2022)**. Disponível em: <https://sol.sbc.org.br/index.php/sbcas/article/view/21646/21470>. Acesso em: 13 out. 2022.

SOUZA, Carlos Affonso Pereira de; OLIVEIRA, Jordan Vinícius. Sobre os ombros de robôs? A Inteligência Artificial entre fascículos e desilusões. p. 65-81. In: FRAZÃO, Ana; MULHOLLAND, Caitlin. **Inteligência Artificial: ética, regulação e responsabilidade**. São Paulo: Thomson Reuters, 2019.

STEIBEL, Fabro; VICENTE, Victor Freitas; JESUS, Diego Santos Vieira de. Possibilidades e potenciais da utilização da Inteligência Artificial. p. 53-64. In: FRAZÃO, Ana; MULHOLLAND, Caitlin. **Inteligência Artificial: ética, regulação e responsabilidade**. São Paulo: Thomson Reuters, 2019.

TEIXEIRA, Tarcísio; ARMELIN, Ruth Maria Guerreiro da Fonseca. **Lei Geral de Proteção de Dados Pessoais: Comentada artigo por artigo**. 3 ed. rev. atual. e ampl. Salvador: Editora JusPodivm, 2021. 208 p.

TEIXEIRA, Tarcísio; CHELIGA, Vinicius. **Inteligência Artificial: aspectos jurídicos**. Salvador: Editora JusPodivm, 2019. 112 p.

TIU, Ekin; TALIUS, Ellie; PATEL, Pujan; et al. Expert-level detection of pathologies from unannotated chest X-ray images via self-supervised learning machine. **Natural Biomedical Engineering**, Set. 2022. Disponível em: <https://www.nature.com/articles/s41551-022-00936-9>. Acesso em: 13 out. 2022.

TUBINO, Luiza Etzberger. **Como os dados pessoais estarão protegidos frente à necessidade de uso destes para o desenvolvimento e uso das inteligências**

artificiais? Tech Compliance. Jun. 2022. Disponível em: <https://techcompliance.org/inteligencia-artificial-e-protecao-de-dado/>. Acesso em: 13 out. 2022.

TURING, Alan M. Computing Machinery and Intelligence. **Mind** 49, p. 433-460, 1950. Disponível em: <https://redirect.cs.umbc.edu/courses/471/papers/turing.pdf>. Acesso em: 13 out. 2022.

TURING, Dermot. **A História da Computação: do ábaco à inteligência artificial**. São Paulo: M. Books do Brasil Editora, 2019. 208 p.

UNIÃO EUROPEIA. Communications from Commission – **Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection** (2020/C 124 1/01). Disponível em: [https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020XC0417\(08\)&from=EN](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020XC0417(08)&from=EN). Acesso em: 13 out. 2022.

VEDOVATE, Shirley Vaz. A inteligência artificial e as transformações no setor da saúde no futuro - A tecnologia na saúde. **Revista Científica Integrada**, UNAERP, v. 5, e. 1, p. 1-21, 2021. Disponível em: <https://www.unaerp.br/documentos/4287-rci-inteligencia-artificial-05-2021/file>. Acesso em: 13 out. 2022.

WANG, Marina. **Eye, robot**: Artificial intelligence dramatically improves accuracy of classic eye exam. *Science - Technology News*. 3 jun. 2020. doi: 10.1126/science.abc4226. Disponível em: https://www.science.org/content/article/eye-robot-artificial-intelligence-dramatically-improves-accuracy-classic-eye-exam?utm_campaign=NewsfromScience&utm_medium=Twitter&utm_source=JHubbard. Acesso em: 13 out. 2022.

WANG, Zhi; LIU, Chaorge; CUI, Xiang. **EvilModel**: Hiding Malware Inside of Neural Network Models. To be appear at 2021 IEEE SYMPOSIUM ON Computers and Communications (ISCC). 5 ago. 2021. Disponível em: <https://arxiv.org/pdf/2107.08590.pdf>. Acesso em: 13 out. 2022.

WEGNER, Gabriela. **Inteligência artificial da Neomed melhora os serviços cardiológicos**. 11 maio 2022. Neomed. Disponível em: <https://neomed.com.br/inteligencia-artificial-da-neomed-melhora-os-servicos-cardiologos/>. Acesso em: 13 out. 2022.

WINSTON, Patrick Henry. **Artificial Intelligence**. Third Edition. Massachusetts, Califórnia, New York, Ontario, etc: Addison-Wesley Publishing Company, 1993.

ZANUTTO, Bruno Gonçalves. **Segurança em Cloud Computing** [s.d]. Disponível em: <https://www.dcomp.ufscar.br/verdi/topicosCloud/Artigo-Seguranca-Cloud.pdf>. Acesso em: 13 out. 2022.

**9. "HOW DARE YOU"? OS LIMITES À LIBERDADE DE INOVAR E OS NOVOS
PARADIGMAS AO ESTUDO DO DIREITO CRIMINAL E DA GESTÃO EM SEGURANÇA
PÚBLICA**

*"HOW DARE YOU"? THE LIMITS TO FREEDOM TO INNOVATE AND THE NEW
PARADIGMS TO THE STUDY OF CRIMINAL LAW AND PUBLIC SAFETY
MANAGEMENT*



<https://doi.org/10.36592/9786554600552-09>

Nathália Igisk Lopes Portugal¹

RESUMO

Em oposição à "tecnocracia", reúnem-se esforços conjuntos de múltiplos saberes, os quais se apresentam como contrapesos à exponencial progressão da incorporação de mecanismos tecnológicos à vida humana. Parte-se do reconhecimento de que, embora úteis e necessárias à evolução e ao aperfeiçoamento humano, as ferramentas não podem ultrapassar sua conotação instrumental, realizando-se por si mesmas, caso contrário se estará subjugando o criador à criatura. Se os processos científicos de inovação se revelarem de maneira transcendente ao desenvolvimento social, absorvendo o homem e não sendo por ele absorvido, demonstra-se a fundamentalidade de ser traçar os limites de sua atuação, freando a emancipação de ferramentas que devem estar a nosso serviço e não contra nós. A análise se dará sobre o confronto Segurança Pública *versus* Inovação, oferecendo a compatibilização entre ambos contra a mútua aniquilação.

Palavras-chave: Veículos Autônomos. Inovação. Segurança Pública. Ponderação. Regulação.

¹ Advogada. Mestranda no Programa de Pós-Graduação da Universidade Federal do Rio Grande do Sul (vinculada ao CDEA). Pós-graduanda em "Direito Penal e Política Criminal" e pesquisadora no Núcleo de Estudos de Direito Penal e Processual Penal Contemporâneos (NEDPP) pela mesma Universidade. Link para o Currículos Lattes: <http://lattes.cnpq.br/8972731121997040>. Correio eletrônico: nathaliaigisk@gmail.com.

ABSTRACT

In opposition to "technocracy," joint efforts of multiple fields are gathered as counterweights to the exponential progression of the incorporation of technological mechanisms into human life. It is recognized that, although useful and necessary for human evolution and improvement, tools cannot exceed their instrumental connotation, doing things by themselves, otherwise the creator will be subjugated to the creature. If scientific innovation processes are revealed to be transcendent to social development, absorbing man instead of being absorbed by him, the fundamentality of setting limits on their actions is demonstrated, restraining the emancipation of tools that should be at our service and not against us. The analysis will be carried out on the conflict between Public Safety and Innovation, offering compatibility between both against mutual annihilation.

Keywords: Autonomous Vehicles. Innovation. Public Safety. Pondering. Regulation.

INTRODUÇÃO

A expansão tecnológica extrapola suas fronteiras científicas e passa a provocar a entrada de outros ramos de estudo ao debate. Já não é novidade a mecanização do setor humano, tampouco o florescimento do emprego de novas técnicas de atuação e desenvolvimento de ordem digital-algorítmica. Tal como toda progressão "evolutiva" de um determinado sistema social - neste caso, dada a introjeção de tecnologias outrora desconhecidas/inexploradas -, a pulverização de ferramentas alimentadas por inteligência artificial e seu notável impacto impõem (e justificam) a necessidade de intersecção científica de outros saberes - sociologia, filosofia, bioética, criminologia, dentre outros. No que concerne especificamente ao direito (já que se trata de artigo jurídico), há consequências significativas tanto no âmbito civil quanto penal, para além de eventual repercussão campo processual e na organização da justiça. Para delimitar o escopo desta pesquisa, a fim de que não exceda os contornos metodológicos impostos, será discutido o grau de intervencionismo tecnológico a partir de uma situação "paradigma" analisada à luz do direito penal sob o viés da imputação/responsabilização penal e os consequentes reflexos à segurança pública.

Com a acelerada incorporação da inteligência artificial a múltiplos segmentos, os estudos humanísticos restam, invariavelmente, aquém, sendo obsoletizados ou relegados a meros devaneios utópicos. Por certo, essa transversalidade não deve ser interpretada como antagonista ao avanço tecnológico, mas como instrumento mediador/moderador entre a ciência analítica e a ciência social, compatibilizando-os. Antes de adentrar, necessariamente, ao exemplo central deste trabalho e - sobre ele discorrer -, é preciso destacar o instituto da "liberdade científica" (previsto no artigo 5º, IX da Constituição Federal), o qual, nesta análise, será vinculado à liberdade de ofício (direito previsto no artigo 5º, XIII da Constituição brasileira), porquanto expressão de uma atividade científica funcional: de desenvolvimento e programação tecnológica. Nesta senda, é também prudente salientar o artigo 218, *caput* e seus §§ 2º e 4º com suas prescrições de fomento à pesquisa e à criação tecnológica. Ocorre que, a liberdade, em qualquer sentido, não é uma prerrogativa ilimitada, encontrando fronteira nos direitos de terceiros, na "lei" moral-social e nos mandamentos da ordem constitucional; em igual perspectiva, a promoção estatal à criação tecnológica não determina a sua "irrestrrição", sendo imprescindível a conciliação entre a sua promoção e a ordem jurídica.

A referência de inspiração para o presente artigo é a incorporação de sistemas veiculares autônomos nas rodovias brasileiras. Já em circulação em outras partes do mundo, por uma série de motivos de ordem estrutural e regulatória tais automóveis não ocupam o sistema viário brasileiro, porém, não deixam de ser uma promessa recente, já que em dezembro de 2020 o Ministério da Infraestrutura emitiu a Portaria 2.663 que incluiu na sua agenda regulatória prioritária a regulamentação dos veículos autônomos sob a Coordenação-Geral de Segurança no Trânsito (CGST). A discussão se assenta em uma raiz filosófica e se desdobra em análises quanto à responsabilização penal e a gestão em segurança pública, uma vez que, i. incita controvérsias sobre o sistema de imputação criminal e ii. aporta aspectos relevantes a serem considerados pelas estratégias públicas em segurança. Quem responderá no caso de dano à integridade física ou à vida de terceiro? Quão vulnerabilizados serão estes terceiros dada a lógica do sistema de autômatos? Quem são estes vulneráveis? Essas indagações - e outras - devem compor a análise para regulação

de questões dessa ordem, que estão imbricadas com a pergunta central do trabalho: qual a liberdade de inovar?

Para desenvolver o conteúdo sugerido no projeto, sobre os procedimentos técnicos à sua formulação: a pesquisa será subsidiada por revisão bibliográfica, com abordagem quantitativa, servindo-se de fontes escritas para embasar seu conteúdo (fontes normativas, doutrinárias e jurisprudenciais; além de pesquisas que contribuam para a consolidação, coerência e compreensão do fenômeno). Quanto a sua natureza, a pesquisa será do gênero básica-aplicada, de matiz exploratório. O método utilizado para o alcance das conclusões finais que se intenciona, será do tipo dedutivo, mesmo que seu ponto de partida seja um fenômeno particular.

É importante, por fim, esboçar a linearidade da proposta para que assim seja possível apresentar sua justificativa, destacar os problemas correspondentes e alcançar seu objetivo. Em um primeiro momento, será feita uma análise sob o prisma constitucional de direitos fundamentais que emergem da tópica; em um segundo, a partir de eventuais consequências determinadas pelo silêncio regulatório, será caracterizado um confronto jus-filosófico (sob a perspectiva criminal) imposto pelo avanço da tecnologia autônoma não senciante.

1 EXPRESSÃO CONSTITUCIONAL DE DIREITOS

O crescente emprego da tecnologia (nos processos humanos - direta ou indiretamente) implica em novos métodos de gerenciamento de risco² a serem administrados pelos entes públicos (por meio de disposições estatais, supraestatais e internacionais)³ e por particulares (através de estratégias de mitigação de riscos e

² Sobre isso, a obra de Ulrich Beck, "Sociedade de Risco" trata sobre a "irresponsabilidade organizada" e as "incertezas fabricadas", enquanto paradoxos da concepção de sociedade pós-moderna, os quais derivam de rápidas inovações tecnológicas, conjugada à incapacidade dos setores estatais em encontrar respostas certas sobre os problemas que se apresentem, gerando temor social (BECK, 2011).

³ Veja: Recomendação sobre a Ética da Inteligência Artificial da UNESCO, publicada em 2022. Disponível em: <https://unesdoc.unesco.org/ark:/48223/pf0000381137_por>. Os Princípios da Organização para a Cooperação e Desenvolvimento Econômico (OCDE) em Inteligência Artificial, adotados em maio de 2019. Disponível em: <<https://oecd.ai/en/ai-principles>>. "O Ato da Inteligência Artificial", proposto pela União Europeia, representando, atualmente, 27 países-membros. Disponível em: <<https://artificialintelligenceact.eu/>>. O qual influenciou o Projeto de Lei 872/21 no Brasil. Os cinco princípios previstos no Projeto norte-americano "para uma Declaração de Direitos em Inteligência Artificial". Disponível em: <<https://www.whitehouse.gov/ostp/ai-bill-of-rights/>>. "A era

danos), formulando-se, assim, uma rede preventiva e protetiva de direitos que, eventualmente, sejam ameaçados pelos avanços tecnológicos. A cada evolução deste sistema "informático", o qual está em perene progressão sob as perspectivas horizontal e vertical do "viver" humano (isto é, quanto ao seu alcance e profundidade), novos desafios são impostos à sociologia e, por fim, ao direito.

O problema-chave desta análise se centra sobre o choque entre duas categorias fundamentais da sociedade contemporânea, incitado pela adoção de veículos autônomos: inovação (científica e/ou tecnológica) *versus* segurança (jurídica, pública e individual - compreendida, portanto, sob um viés alargado). Pode-se afirmar que a correlação entre as duas variáveis é complexa, não sendo possível concluir, categoricamente, que a solidez de uma acarrete a deficiência da outra (e vice-versa), tampouco que tenham correspondência proporcional; isso porque, diferentemente de outros fenômenos sociológicos e jurídicos apreensíveis, o exame de probabilidade sobre novas tecnologias e suas consequências é infinito, abrangendo desde casos possíveis a utópicos, com múltiplas implicações jurídicas.

Dada a dificuldade de segmentarização do problema, que se dá pela própria "ontos" da tecnologia (versatilidade, progressão e amplitude), é necessário estabelecer um diálogo sociológico sobre o que se pretende prevenir e remediar com a regulamentação das práticas de inovação⁴; vale dizer, sob uma perspectiva do direito, observá-la enquanto pauta de nova conflitualidade⁵ decorrente dos

da interdependência digital: relatório do Painel de Alto Nível em Cooperação Digital do Secretário-Geral das Nações Unidas" que traz uma série de outras recomendações. Disponível em: <<https://digitallibrary.un.org/record/3865925>>.

⁴ "Esta lógica de priorização não está dissociada também do aspecto relacionado à inovação, que tem no retorno privado um de seus alicerces conceituais se retornarmos à Schumpeter, mas não pode estar dissociada de retornos sociais, sob pena de o crescimento decorrente deste processo inovativo, ínsito ao capitalismo, não ser sustentável e sobretudo não alcançar a maior parte das pessoas, como adverte Stiglitz (2016). Para tanto, a atuação estatal é impositiva, especialmente por meio da regulação para efetuar os condicionamentos e controles necessários. De algum modo, um projeto político de superação do subdesenvolvimento, para novamente citar Furtado (2013), deve ter um amplo conhecimento da realidade, envolver um certo consenso social (diante da necessidade de confrontar padrões de poder estabelecidos), sem nunca prescindir da pesquisa e da produção de conhecimento – que estão na base da inovação e que já eram, quando dos escritos de Furtado, e continuam sendo, elementos indispensáveis para uma guinada inclusiva do país." (RODRIGUES, 2021, p. 189).

⁵ Termo utilizado pelo sociólogo José Vicente Tavares, alcunhado em diversas de suas obras (refere-se aqui a "Violências e Conflitualidades") para explicar os processos de violência da sociedade contemporânea, centrada na era do globalismo. Transporta-se esse conceito para questionar a institucionalização da violência caso não se dê as delimitações cabíveis à inovação.

processos de globalização. A partir da disrupção de uma sociedade tradicional para uma sociedade contemporânea, estabeleceram-se muitas discussões acerca das modificações tecnológicas, as quais, pelo transcurso do tempo, sucumbiram à obsolescência, dando lugar a alterações ainda mais intrincadas. Quer dizer, do mesmo modo que a tecnologia progrediu de operações simplórias a mecanismos de inteligência artificial⁶, expandiram-se os casos de interesse jurídico (quantitativa e qualitativamente) a seu respeito.

Sobre o direito penal em foco, questionam-se os riscos derivados dos sistemas de inteligência artificial (forte ou fraca)⁷ à salvaguarda de direitos tutelados (especialmente nos casos de violação à incolumidade física e de risco à vida). Porém, não só ao âmbito penal incumbe balizar o alcance da tecnologia; para intentos preventivos, é também tarefa da bioética arrefecer a liberdade irrestrita deste campo, mesmo que a custo de certas inovações científicas⁸; e não só, compete, igualmente, à sociologia explorar estes novos aspectos criminológicos para bem subsidiar o direito no confronto de casos complexos.

Em que pesem as mesmas motivações dos outros modais de transporte, **os cenários que envolvem a direção de veículos automotivos são sensivelmente mais complexos, em razão do número de variáveis a serem consideradas.** As condições das vias, os pedestres, a quantidade de outros veículos e motoristas, os ciclistas, os animais e o tráfego fazem do desafio de conduzir autonomamente um carro em segurança para si e para o ambiente **algo muito complexo de ser modelado.** (FRIDMAN et al., 2017 *apud* GUEDES, 2019, p. 49) (grifos nossos).

Ciente de que não há como exaurir o plexo de contingências que desafiam os sistemas regulatório e jurídico pelos processos de inovação, pretende-se extrair uma

⁶ "todo sistema computacional que simula a capacidade humana de raciocinar e resolver problemas, por meio de tomada de decisões baseadas em análises probabilísticas". (FRAZÃO, 2019, p. 06).

⁷ A inteligência artificial forte opera em domínios diversos e busca simular a inteligência humana (abrangendo-se a "*machine learning*", que possui capacidades de autoaprendizagem e pode, portanto, tomar decisões autônomas independentes, realizando interferências não esperadas/programadas) podendo performar em contextos inexplorados e desconhecidos; a inteligência artificial fraca, por sua vez, tem por escopo realizar tarefas específicas, atuando conforme os limites dados na sua programação (HIDALGO, 2021, p.15).

⁸ Observe-se, por exemplo, a Lei nº 11.105/2005 que em seu artigo 6º, inciso IV veda a clonagem humana, tendo em vista, dentre outros fatores, a vedação à eugenia humana (HABERMAS, 2004).

conclusão abrangente a partir da manifestação concreta de um problema. Aqui, então, reportar-se-á à disponibilização de automóveis operacionalizados por inteligência artificial como exemplo central, para enfim ser demonstrada a relevância do dilema suscitado acerca da liberdade criativa. Para atender a este propósito, é necessário, inicialmente, fazer uma breve conversão à discussão sobre direitos fundamentais para enfim lançar-se à investigação das bases legitimantes da controvérsia posta.

Sendo a observação dos potenciais danos advindos da "tecnologização desregulada" uma questão genérica (do cível ao crime), é necessário compreender o instituto a partir de sua natureza jurídica, para então apresentar soluções aos problemas que dele possam advir. Em razão da tecnologia, expressam-se dois mandamentos constitucionais: i. O instituto da "liberdade científica", dado no artigo 5º, inciso IX da Constituição Federal; ii. O fomento à pesquisa científica, à criação tecnológica e à inovação, conforme prescrito no artigo 218, *caput* e parágrafos subsequentes da Constituição Federal (todos inseridos pela Emenda Constitucional nº 85 de 2015).

Considerando que a dita liberdade científica (artigo 5º, IX da Constituição Federal) se realiza pela liberdade de ofício (artigo 5º, XIII da Constituição Federal), para que se atenda o mandamento constitucional de inovação (artigo 218 da Constituição Federal), percebe-se que há a manifestação de um direito fundamental implícito (liberdade de inovar) que é "meio" para realização do que está explícito no catálogo da Constituição. Assim sendo, se o Estado encartou a fundamentalidade do incentivo à inovação, a qual se realiza através da liberdade científica e profissional do seu desenvolvedor/pesquisador, o que poderia confrontar esse instituto para tentar mitigá-lo? Para este trabalho, não *basta* que tal pergunta seja respondida pelos diversos casos concretos que demonstrem a necessidade de regulações mais concretas, pois se pretende lançar luz ao que, por subjazer a todos esses fenômenos, respalda - unissonamente - a mobilização estatal.

1.1 Uma questão de ponderação

Os desafios impostos ao direito pela incorporação da tecnologia aos processos humanos se desdobram do caráter inovativo inculcido a ela, confrontando a estabilidade social e os parâmetros jurídicos vigentes. Porém, não é em nome de uma segurança jurídica infalível e à conservação social engessada que se obstará o progresso humano, o qual está, indiscutivelmente, atrelado ao desenvolvimento científico e tecnológico. O risco é intrínseco à dinâmica humana, mas há parâmetros de conformação socialmente consentidos e incorporados como tais pelo Estado, os quais determinam que, em caso de eventuais excessos que desbordem as fronteiras desse risco permitido, haja a imprescindível intervenção da Administração Pública para colmatar as lacunas sistêmicas.

É a partir da identificação de uma situação que opere além do risco permitido, vulnerando sobremaneira outros bens jurídicos estabelecidos, que faz acender a indispensabilidade da correção jurídica ao problema. O próximo passo é estabelecer *como* o direito trabalhará a temperança entre a proteção de um determinado bem em confronto a outro constitucionalmente protegido. Parte-se de uma análise de limite dos direitos fundamentais⁹, prossegue-se a ponderação¹⁰ entre bens conflitantes (mecanismo eleito para dirimir as incompatibilidades no confronto de bens adversos) e, deste exame, alcança-se um resultado o qual se corporificará por meio de medidas oficiais. *In casu*, o espectro de implicações suscitados pela tecnologia impõe um estudo segmentarizado de cada âmbito jurídico, de maneira que, como já suscitado, não é possível fazer provisões para cada aspecto relevante ao direito - muito embora a justificativa fundante seja símile a todos -, o que explica por que o pontapé deste trabalho foi dado com base em paradigma específico.

⁹ "Tendo sempre presentes tais premissas, é possível compartilhar do entendimento de Klaus Stem, no sentido de que uma separação clara entre o âmbito de proteção dos direitos fundamentais e suas limitações, assim como das possibilidades de limitação e os limites por sua vez postos à limitação dos direitos, não é apenas relevante para uma dogmática "límpida" dos direitos fundamentais, mas também assume importância para o manejo apropriado, especialmente por parte da jurisdição constitucional e do legislador, das normas de direitos fundamentais" (SARLET, 2018, p. 406).

¹⁰ "A posição dos direitos fundamentais - que não podem ser considerados uma espécie de super-codificação relativamente ao restante da ordem constitucional deve, nesse contexto, ser analisada à luz do princípio da unidade da Constituição, resolvendo-se os inevitáveis conflitos por meio dos mecanismos de ponderação e harmonização dos princípios em pauta" (SARLET, 2018, p. 75).

Antes de adentrar ao juízo de ponderação propriamente dito, é preciso apontar qual o direito fundamental, *in casu*, que se manifesta contrariamente à liberdade incondicional de fomento à pesquisa. Dado que o caráter utilizado nesta pesquisa se deu sob um viés social-criminológico, em razão da vulneração física de outrem graças à tecnologia incorporada em veículos autônomos, pode-se dizer que, em última análise, a questão se assenta em uma perspectiva imbricada à salvaguarda da Segurança Pública¹¹ (artigo 144 da Constituição Federal), a qual vem instrumentalizada pelos ditames criminológicos, penais e processuais penais. Sendo que o dilema se instaura nesse cenário, é inevitável conhecer o que tais ramos científicos oferecem, dogmaticamente, à conclusão do impasse - assim como, é fundamental entender como suas fronteiras de atuação contribuem à complexificação da resolução.

Para a coesão deste artigo científico, é primordial referir a elaboração não ortodoxa do seu conteúdo. Vale dizer, embora o que tenha motivado a introdução do assunto em apreço se origine da constatação de um novo fenômeno social relevante, é a comprovação de sua aptidão à intercessão do direito - porquanto fundamentais os mandamentos jurídico-hermenêuticos para o cotejo apropriado entre categorias aparentemente conflitantes - que justifica o conteúdo da pesquisa. Desse modo, distanciou-se do caso paradigma para atingir-se o âmago de justificação de sua relevância ao direito, demonstrando-se que, dada a existência de uma concepção de risco permitido (em relação a um determinado bem ou direito), aquilo que o extrapole deve ser devidamente corrigido. Assim, assumindo-se que ditas correições só encontrem legitimação em conteúdo estatal (através de previsões regulatórias alicerçadas sob o Princípio da Proporcionalidade¹², que se assenta no binômio

¹¹ Veja-se a obra de Denninger (1990, p. 225-226), na qual redescobrem-se "novos" direitos - portanto, justificando-os - dentre eles, a segurança pública.

¹² "Outra limitação importante para uma compreensão e aplicação constitucionalmente adequada do conceito material dos direitos fundamentais diz respeito à necessária harmonização entre os direitos "revelados" pelo intérprete e a sistemática da Constituição. Assim, deve-se atentar para a problemática que diz com a forma de incorporação ao direito interno e a posição hierárquica dos direitos fundamentais de origem internacional (e até mesmo legal, para aqueles que os admitem), uma vez que os rumos a serem tomados dependem, em última análise, do posicionamento a este respeito. Mesmo que se outorgue aos direitos sediados em tratados internacionais posição equivalente aos direitos fundamentais constitucionais, a solução jamais poderá ser a de sacrificar um dos direitos em rota de colisão, aplicando-se, nesse particular, as regras de praxe, procedendo-se à ponderação dos valores em pauta, à luz do princípio da concordância prática e da proporcionalidade" (SARLET, 2018, p. 146).

proibição do excesso x proibição da insuficiência), faz-se necessário apresentar as variáveis apreciáveis à composição da produção legal-regulatória exigível.

Considerando o caso empiricamente relatado, pode-se afirmar que estamos defronte à dicotomia "inovação *versus* segurança", cuja essência desponta em um juízo de harmonização sistêmico entre bens que poderá, ou não, resultar em uma nova normativa prescritiva. Tendo-se em conta que o conceito de inovação científico-tecnológica se exaure em si mesmo, volta-se, necessariamente, à concepção de segurança para destrinchar aquilo que a compõe. Antes de prosseguir, destaca-se que esta é uma proposição inicial não exauriente, ou seja, nela são dispostas algumas das concepções mínimas para o concertamento de uma estrutura estatal voltada ao fim "segurança pública". À primeira vista, então, elencam-se como primordiais à conceptualização e à orientação deste bem constitucional previsto no artigo 144 da Constituição Federal, as determinações concernentes aos direitos penal e processual penal, assim como à criminologia.

A partir dessa identificação, deverá o Estado questionar se os conteúdos já dispostos no Ordenamento dão cabo à promoção e preservação da segurança ou se são insuficientes à proteção aclamada. Para essa investigação, faz-se oportuno o estudo da disciplina penal posta - já que de conteúdo material -, verificando seu grau de capacidade à tutela da segurança pública. Desse modo, parte-se ao próximo capítulo, onde serão analisados os critérios à imputação penal e as dificuldades que dela emanam.

2 NOVA CONFLITUALIDADE

O fenômeno social que conduz às premissas anteriormente sedimentadas, desdobra-se da adoção de mecanismos de inteligência artificial pelas empresas automobilísticas, as quais disponibilizam veículos classificados nos níveis 4 ou 5 de autonomia¹³, ou seja, que dispensam completamente a intervenção humana em seus trajetos. A ideia por trás deste recurso é preservar a vida de quem esteja no interior

¹³ "Classificação criada pela *Society of Autonomous Engineers* (SAE), sociedade de padronização de *standards* baseada nos Estados Unidos, e depois utilizada pela *National Highway Traffic Safety Administration* (NHTSA), autoridade federal de trânsito deste país, para ordenar os níveis de autonomia de carros autônomos" (ENRICO ROBERTO, 2021, p. 128).

do veículo em detrimento de vidas externas, caso essas representem uma ameaça (em conjunto com outros fatores ambientais) aos tripulantes do automóvel, a partir de técnicas de engenharia aplicadas ao produto.

O questionamento trazido é: além de um conflito moral subjacente ao evento ("Dilema do Bonde"¹⁴), se estaria vulnerando excessivamente a integridade física de uns em nome de outros? Isto é, dada a possibilidade inicial de salvamento de terceiros (transeuntes, motoristas e "caroneiros") de um potencial acidente de trânsito, com esta ferramenta de inovação se estaria restringindo ou cindindo, antijuridicamente, tais chances de escapatória? Poderia se falar em desvalor de uma vida sobre a outra, tão só porque Tício adquiriu algo que Mévio não? Essas não são respostas simples. É sabido que máquinas processadas através da inteligência artificial realizam a análise combinatória dos múltiplos fatores identificáveis em um potencial acidente de trânsito, algo impossível de ser realizado por humanos ao volante. Logo, elas seriam capazes de adotar a "melhor"¹⁵ manobra em um evento que demande respostas rápidas, por esse motivo apresentariam-se como artífice benéfico ao trânsito.

Contudo, quando avançamos nos estudos concernentes às inteligências artificiais, percebemos que há problemas advindos da sua fonte de alimentação cognitiva: os algoritmos¹⁶. Segundo Frank Pasquale (2005), vive-se uma *black box society*, na qual algoritmos decidem quem somos, o que pensamos, o que queremos, bem como quais os nossos direitos, as nossas perspectivas e expectativas de vida. E o problema não advém apenas da opacidade algorítmica, mas do modo como ela se operacionaliza - ressaltando-se, por exemplo, que já foram identificados padrões

¹⁴ É um experimento de pensamento em ética, idealizado pela filósofa Philippa Foot em 1967, com diversas variantes propostas por outros filósofos que analisaram o tema desde então.

¹⁵ Conforme BRYNJOLFSSON e MCAFEE (2016) - *in* MELLO, LAZARI (2022, p. 129) - busca-se a "melhor solução possível". Porém, questiona-se: a melhor solução possível sob qual paradigma ético-filosófico? Kantiano? Utilitarista? Em qualquer caso, haveria realmente essa predisposição subjetiva à máquina ou ela operaria no melhor interesse de quem está dentro do veículo? Considerando que é um dispositivo adquirido, é *difícil* crer que funcionaria de outro modo, a despeito do beneficiamento dos seus integrantes.

¹⁶ Segundo Cormen (2013, p.1), um algoritmo computacional contém passos descritos de maneira suficientemente precisa para que o computador seja capaz de entendê-lo e consiga executar determinada tarefa.

discriminatórios nas bases de dados de diversas máquinas autônomas e em diversas operações¹⁷.

De modo que, convém resgatar o que Habermas descreveu na sua obra "O Futuro da Natureza Humana: a caminho de uma nova eugenia liberal?": o temor da expansão da tecnologia como tecnologia, ou seja, enquanto técnica que se coloca não como meio para o avanço, mas como fim. Até onde a tecnologia não está invadindo a forma de vida do ser humano, de modo que as concepções de liberdade e ação política são colocadas *em jogo*, em nome e em favor de uma espécie de razão instrumental¹⁸ que é incapaz de deliberar sobre temas sensíveis à humanidade? Daí emerge a problemática filosófica suscitada: é razoável que máquinas resolvam e encerrem um dilema moral-filosófico, decidindo quem vive e quem morre?

Mais, estaríamos diante da formação de uma nova conflitualidade dada à vulnerabilização generalizada de múltiplos atores sociais¹⁹? É a dogmática penal insculpida em nosso sistema o bastante para controlar potenciais danos, através da imputação de responsabilidade ao "causador"? Como será visto, a configuração da responsabilização penal *contribui* para a formação desta brecha no sistema de Segurança Pública, assim, é preciso encontrar quais caminhos seriam hábeis para a conformação entre inovação, sociedade e direito, para que não sejamos subjugados por um Ordenamento anômico e frágil.

2.1 Onde está o Direito Penal?

Deve-se, desde já, para progressão correta deste trabalho, rechaçar eventual responsabilidade da máquina em si (levando-se em consideração os ensinamentos da dogmática penal atual quanto ao conceito de ação/conduta *x* mero evento naturalístico), de modo que, resta-nos abordar: i. a eventual responsabilização do programador ou do usuário, bem como, ii. as regulações e práticas preventivas

¹⁷ Para entender a abrangência dessa discriminação, recomenda-se: MENDES, 2019, e BUOLAMWINI; GEBRU, 2018.

¹⁸ Nesse sentido, Cathy O'Neil (2016) afirma que apesar de terem uma reputação de imparcialidade, esses modelos computacionais, e, por consequência, os algoritmos, "refletem objetivos e ideologias".

¹⁹ A título exemplificativo, veja-se os casos finamente relatados em MELLO e LAZARI (2022, p. 132-133), que explicam os riscos oriundos de erros de programação oriundos de inteligência artificial.

observáveis para fins de política criminal. Ambas reflexões estão apoiadas na análise de incremento do risco de lesão e/ou dano gerado pela liberdade de inovar.

A pesquisa se inaugura da percepção empírica de vacância regulatória delimitante das inteligências artificiais, com desdobramentos na seara criminal sob a ótica da responsabilidade penal a partir de acontecimentos operacionais. Frisa-se o termo "acontecimento", pois "ação" e "conduta" são aspectos inerentes ao comportamento humano. Como a estrutura desse fato não pode ser entendida sob a lógica de um mero evento naturalístico - já que ele está assentado num comportamento humano pré-existente de programação - é útil recordar a Teoria da Ação Significativa (pensada pelo Professor Tomás Salvador Vives Antón e desenvolvida no Brasil, especialmente, por Paulo César Busato). Ela preconiza que "ações" são configuradas de acordo com seu significado social (pelo contexto em que se produzem), de modo que haja sua interpretação com base no disposto em regras e normas (BUSATO, 2013, p. 252).²⁰ O que uma máquina produz é acontecimento e não ação, mesmo que não seja a expressão de um evento naturalístico, pois a interpretação jus-social das "ações" dela derivadas são compreendidas como não voluntárias. Logo, essa diferenciação se alinha à Teoria do Delito²¹, a qual não vislumbra a existência de crime sem comportamento humano (comissivo ou omissivo), de modo que, o mero acontecimento não implica em conteúdo jurídico-criminal, embora a conduta que o subjaz (praticada pelo programador) sim.

Se "acontecimento" é o que deriva dos exercícios operados pela máquina dotada de inteligência artificial, justifica-se a impossibilidade de hipotetizar a sua responsabilidade penal (considerado qualquer prisma de inteligência artificial - fraca ou forte), ao menos, até que atinjam o mais alto nível de liberdade, em que se constata

²⁰ Ela se deve a uma pragmatização da compreensão de fenômenos jus-filosóficos, a partir da acepção desenvolvida por Ludwig Wittgenstein e a linguagem, encontrando respaldo na Teoria do Discurso entendida por Habermas na interpretação de direitos fundamentais ("para solucionar o paradoxo da legitimidade oriunda da legalidade" - LUDWIG, 2013, p. 53).

²¹ "Ainda que prevaleça, atualmente no direito brasileiro, a aplicação da teoria finalista da conduta, não se desconhece a existência de outros modelos de conceituação de ação, cada um deles correspondendo à evolução da ciência de seu tempo e variando conforme as condições materiais da sociedade como o modo de produção econômica, as concepções filosóficas, jurídicas e institucionais, dentre várias outras circunstâncias." (TAVARES, Juarez. **Fundamentos da teoria do delito**. Florianópolis: Tirant lo Blanch, 2018. *apud* MELLO; LAZARI [p. 126, 2022]).

a existência de funções cerebrais superiores: percepção sensorial, a capacidade de sentir dor, o senso de ser, a autodeterminação e a consciência (CICUREL, NICOLELIS, 2015, p. 26)²². Com essa premissa sedimentada, justifica-se que as indagações contidas nesta pesquisa estejam voltadas ao papel do direito penal enquanto eixo de manifestação das intenções estatais, visto que, o seu catálogo de dispositivos de controle (por meio da dogmática de imputação) não é capaz de dirimir a problemática, como se verá a seguir.

Se os sistemas autônomos ainda não são capazes de conduta no sentido penal, atesta-se a irresponsabilidade das máquinas pelas suas operações. Agora, inaugura-se a discussão sobre a responsabilização dos desenvolvedores e usuários (sob a égide da responsabilidade subjetiva - corolário do direito penal) no caso de lesão a terceiro. Ela é compreendida através da correlação: "ação culposa" - *lato sensu* (onde se analisa a autoria por critérios de causalidade) → "resultado" → "nexo de causalidade" → "imputação" (responsabilização). Por vezes, é nebulosa a tarefa de determinar a imputação ao crime perpetrado, após aferida a autoria. Essa análise de imputação circunda aspectos, à primeira vista, não identificados, como: a autocolocação em perigo, a heterocolocação em perigo consentida, o fim de proteção da norma, a evitabilidade, a omissão imprópria e o incremento do risco permitido (GIMBERNAT, 2019). São os dois últimos elementos que encerrarão o debate dogmático penal sobre a tópica.

Ao se dirigir à responsabilização dos desenvolvedores (para qualquer caso), tem-se às mãos um estudo obscuro, justamente pela gama de profissionais envolvidos na elaboração de certa tecnologia. Associa-se a este outro fator complicador: quando possível a tomada de decisão independente pela inteligência artificial, muitas serão "opacas"/"inteligíveis" (*black box* da inteligência artificial), não podendo ser visualizado onde ocorre o processamento do sistema (Knight, 2018), de modo que, inviável o lastreio do caminho tomado pelos "neurônios" do sistema para se saber o porquê de tal operação (e se houve algum vício na programação - conduta culposa imputável).²³ Também, destaca-se que há uma produção difusa dos

²² Talvez, direcionando-se ao sentido de saber absoluto proposto pela filosofia Hegeliana?

²³ "O Projeto de Lei nº 2018/49 da cidade de Nova Iorque, Estados Unidos, consiste em estabelecer diretrizes para a criação de mecanismos de transparência em tais sistemas (The New York City Council, 2018), exatamente para facilitar a percepção de elos causais e permitir *accountability* pela

sistemas de inteligência artificial que se dá pela disponibilização de *softwares* livres (desparametrizados), sobre os quais os programadores podem desenvolver seus próprios sistemas, tornando inócua a tentativa de determinar qual fator contribuiu para as falhas de determinado projeto.

De qualquer forma, eventual responsabilização do desenvolvedor se daria no bojo dos crimes por omissão imprópria (e análise de evitabilidade) derivada de uma posição de garante (dever de cuidado objetivo). No caso dos usuários, abre-se a mesma possibilidade de imputação, só que a partir da análise do *mau uso*, isto é, se o condutor desvirtua culposamente o objetivo do sistema ou deixa de assumir sua posição de garantia nos procedimentos que lhe compete. Se essas ações humanas implicarem em um resultado subsumível ao suporte fático da lei penal, justifica-se a responsabilização criminal, como em qualquer outro caso de imputação desta natureza; logo, não há novidades quando o tema é tratado sob essas duas perspectivas, pois observáveis os ditames penais gerais de imputação e exclusão da responsabilidade. Por isso - e por causa disso -, o desafio se dá justamente sobre: i. Os casos em que não há ação disponível ao condutor para evitação do dano²⁴ e, ii. A dificuldade na responsabilização do programador - não só porque os processos operacionais são obscuros - por que se esvaziaria por completo as iniciativas de autonomização das máquinas no caso de eventual responsabilização (para fins de prevenção geral) daquele que observa a *lex artis*.²⁵

Como alertado anteriormente, do caso paradigma utilizado para inaugurar o debate se prolongam importantes ramificações que estão sob a égide do direito -

sua implementação e uso (ROBERTO, 2021, p. 127)". No Brasil, tem-se: a Portaria MCTI nº 4.578/22, e os PLs: 5051/19, 21/20 e 872/21. Em março de 2022, uma comissão formada principalmente por juristas foi estabelecida para debater a questão da inteligência artificial. Como resultado dessas discussões, foi entregue um texto Substitutivo sobre os projetos de lei em questão ao Presidente do Senado, com o objetivo de auxiliar na avaliação dessas propostas legislativas. O Relatório Final desse texto foi aprovado em 06 de dezembro de 2022 e apresenta uma abordagem sobre os limites éticos da utilização da inteligência artificial.

²⁴ "(...) os agentes inteligentes avaliam autonomamente as informações tomadas do seu entorno e reagem ao produto dessa avaliação sem uma influência humana, de forma a cumprir de forma ótima a missão que lhes foi assignada (...) Isso quer dizer que uma certa imprevisibilidade dos agentes inteligentes e o correlato risco para terceiros é como que 'pré-programada'." (KARNOW, 1996, p. 55 in MELLO e LAZARI (2022, p. 139).

²⁵ E veja, resolver a responsabilidade do ato lesivo pela aplicabilidade de um presumível estado de necessidade exculpante é questionável. Isso porque é o programador que insere a regra no sistema o que não se equipara à situação do condutor humano que tem de tomar uma decisão em face da eclosão imprevisível da situação dilemática.

como a análise dos direitos fundamentais. Reconhecido que o fenômeno suscita questões de Segurança Pública, foi necessário estabelecer um juízo de ponderação entre este direito e outro, qual seja, a Liberdade de Inovar. Para tal, adentrou-se à dogmática penal para examinar se seu conteúdo seria suficiente à salvaguarda da Segurança neste contexto. Concluiu-se pela inoperância das prescrições vigentes para o gerenciamento do caso, dadas as complicações de atribuição de responsabilidade criminal aos eventos em que ela não consegue ser auferida pelos padrões da imputação objetiva²⁶. Assim, finaliza-se sob a concepção de que a disciplina penal se apresenta, *in casu*, como válvula de promoção à elaboração de conteúdos eficazes a responder o impasse jurídico trazido, já que ao fenômeno subentendem-se temas de cunho social-criminológico, os quais, caso forem reconhecidos, serão posteriormente incorporados à própria disciplina penal para sua proteção²⁷. Sem o reconhecimento desse constructo jurídico, incorreremos ou:

a) Na repetida "solução" ao problema através das compreensões de imputação criminal já observáveis pelo Ordenamento, pois eficazes àquela gama determinada de situações²⁸. Se a *mera* análise de imputação fosse suficiente, não haveria um efetivo problema a ser discutido. Porém, reconhecendo-se que os critérios dispostos no Direito Penal são insuficientes para insculpir o âmbito de desaprovação do Direito (até mesmo acentuando tal dificuldade), é preciso ir além,

²⁶ E aqui, demonstra-se a utilidade da adoção dessa concepção como complementar - já que compatível - ao Sistema Penal Finalista adotado no Brasil, uma vez que ela fornece critérios suplementares hábeis ao enfrentamento de casos complexos, pois, ainda que não seja capaz de encerrar a questão, escancara a deficiência dos padrões dogmáticos para resolvê-la.

²⁷ Configurando o conflito entre a liberdade científica, que é exercício de liberdade individual, e a dignidade da pessoa humana, em última análise. Dois princípios de ordem pública em conflito, o que torna necessário estudar formas de dirimi-lo, sem frear inexoravelmente as investigações tecnológicas e nem causar uma abertura de parâmetros abusivos para a pesquisa em nome de um certo "interesse científico".

²⁸ "(...) podemos perceber que a mesma força teórica encontrada no 'cuidado' heideggeriano, leva o fundamento onto-antropológico do direito penal - aberto à historicidade e, portanto, marcado pelo inacabamento - a se servir da condição de 'ciência procurada' [*episteme zetoumene*]. A incompletude, aqui, não é uma deficiência, mas um modo de ser que possibilita o aprimoramento contínuo, pelos mais diversos caminhos teóricos, a lembrar que 'tudo é caminho' [*Alles ist Weg*]. Sem essa consciência corremos o risco de nos tornarmos 'papagaios' de teorias, que - ao simples e incansavelmente repetir, consagrando o 'mesmismo' - mortificam as maiores bondades das melhores compreensões, quais sejam, as possibilidades teóricas de conjeturar novos horizontes. Esses novos horizontes poderão acenar para outras perspectivas de inovação na dogmática jurídico-penal. Mas a tomada dessa consciência exige que nos afastemos das zonas de conforto teórico, aquelas que nos desobrigam a pensar, já que dispomos de um autor que por nós pensou." (TEIXEIRA NETO, 2021, p. 32-33).

percebendo no âmbito Criminal a capacidade apriorística de reprovação de condutas para influenciar as vindouras tomadas de decisão pelo Ordenamento (através de seus regulamentos).

Ou ainda,

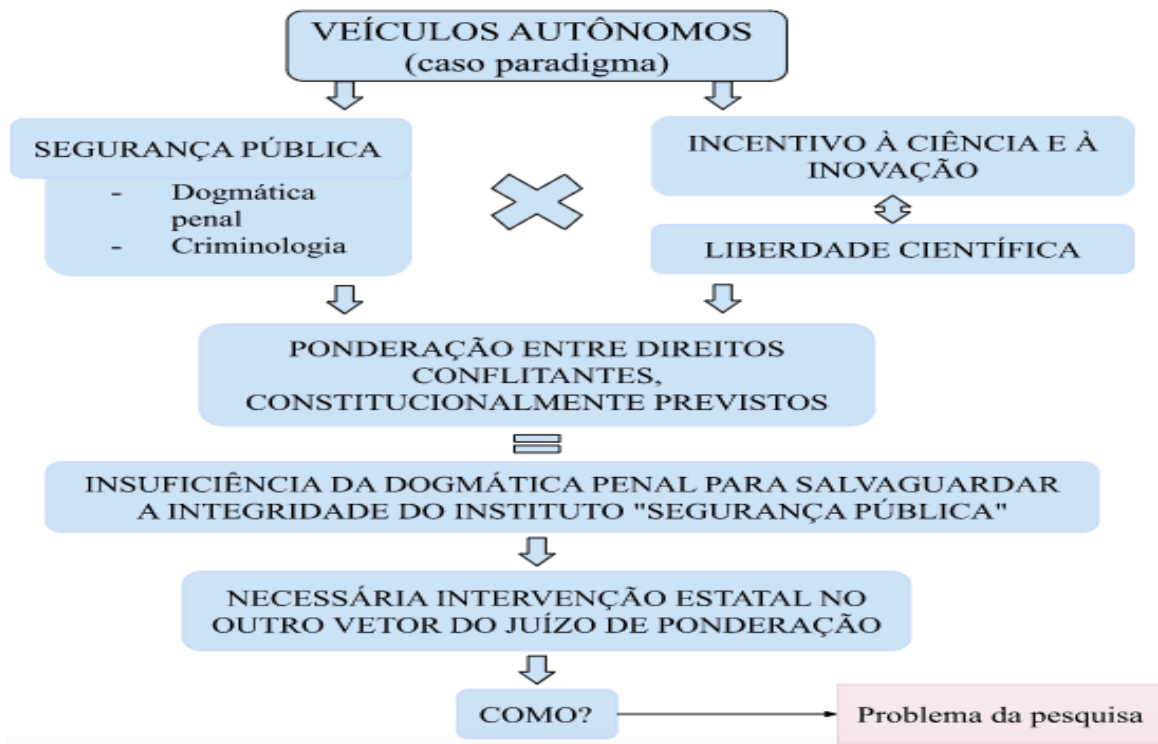
b) Na impropriedade de tratar conteúdos afeitos ao direito penal por meio de instrumentos disponíveis à seara civil - pois, como ao direito não é permitida abstenção, uma vez que, o que o legitima é a *capacidade* de correção social -, desvalorizando-se os bens jurídicos postos em questão.

A primeira característica do CTB é a tipificação de uma série de crimes de trânsito em seus arts. 302 a 312, tais como o homicídio e a lesão corporal culposos na direção de veículo automotor. Tendo em vista a extensão do rol de crimes previstos, muitos casos de responsabilidade civil acabam tendo sua discussão de alguma forma fixada ou pautada pela apreciação havida em juízo criminal. É evidente que, sendo a responsabilização criminal personalíssima e estritamente dependente do elemento volitivo (culpa), com menos espaço para criação jurisprudencial, e sendo todos os crimes previstos no CTB, exceto o do art. 310,8 direcionados a condutores (humanos) de veículos, **a inserção de carros sem motoristas pode deixar lacuna importante na legislação penal, cuja gravidade repressiva importa no sentido de desestimular a ocorrência dos fatos típicos em questão.** Isso pode ser relevante para a apreciação de casos de responsabilidade civil, não só porque se perde a baliza do juízo penal, com sua maior exigência de nível de prova e perícia, **mas também porque as normas de responsabilidade civil podem subitamente se tornar as guardiãs mais diretas dos bens jurídicos – ou, no jargão civilista, da prevenção dos danos – atualmente tutelados por dispositivos criminais.** (GUEDES, 2019, p. 30-31) (grifos nossos)

3 LIBERDADE DE INOVAR: até onde se pode ir?

Para ingressar no capítulo final e na derradeira conclusão deste artigo, é primordial elucidar a concatenação de ideias utilizada, a fim de que a proposta aqui contida faça sentido. Comprometendo-se com o dever de projeção do problema de pesquisa - a

fim de que seu resultado não tenha só justificativa, mas *respaldo* -, será traçado o esqueleto de execução deste projeto em um fluxograma:



Valeu-se de um caso concreto para justificar a importância da análise constitucional de direitos aparentemente colidentes: segurança e inovação. Após, promoveu-se um juízo ponderativo entre ambos, investigando se os mecanismos à disposição para sua salvaguarda são o bastante para tal. Dado que o conceito de fomento à inovação se *cumpr*e por si mesmo - ainda que dependente de ações práticas para este fim -, centrou-se no exame do conteúdo jurídico que *realiza* as opções estatais de reprovação, isto é, na dogmática penal, com objetivo de perscrutar sua capacidade de manutenção do sistema de Segurança Pública vigente. Voltando-se ao direito penal, compreendeu-se que a categoria de responsabilização prescinde a qualquer tentativa de imputação às máquinas autônomas (ação *versus* acontecimento), de modo a restar a potencial responsabilidade do programador e do usuário. Como há o critério subjetivo de culpa inerente ao conteúdo da "ação penal", percebeu-se a dificuldade em estabelecer a imputação desses agentes - seja pelos obstáculos intrínsecos à operacionalização da inteligência artificial, seja pela

complexidade da verificação de culpa ou ainda, pela não-recomendabilidade deste encartamento, sob pena de serem punidos agentes prudentes²⁹.

Se não há o que possa conservar a higidez do sistema de segurança frente aos ditos avanços tecnológicos, impõe-se a necessária ingerência estatal na, até então incondicionada, liberdade profissional de inovar, pois é deste absolutismo que afloram as arestas do Sistema de Segurança Pública. Aqui, impõe-se o ponto fulcral desta pesquisa, onde se abre espaço para conjecturar o *modo* de atuação do Estado sobre a irrestrição da inovação tecnológica. Não se pretende, porém, encontrar soluções cabais ao problema, mas apontar considerações jurídico-constitucionais-criminais interligadas que precisam ser contempladas/respondidas pelo modelo eleito de interveniência estatal.

De quem será a responsabilidade no caso de acidente de trânsito fatal ou lesivo à saúde de terceiro, nos casos em que não seja viável/possível a aferição de ocorrência de omissão imprópria do programador ou usuário? Isto é, comprovado o afastamento de responsabilidade dos agentes pela análise dos critérios de imputação criminal *tradicionais*, o que o Estado brasileiro dispõe para repressão dos efeitos desse tipo de tecnologia? Se não dispõe de conteúdo suficiente para corrigir as consequências da incorporação desse modelo veicular em solo nacional, o que deverá ser considerado quando do estabelecimento das condicionantes para tal - em outras palavras, o que deverá a Coordenação-Geral de Segurança no Trânsito (CGST) contemplar antes de regular sobre autômatos?

Já que, quando alcançado o momento de avaliação da proporcionalidade entre direitos (segurança e inovação), percebeu-se que um dos sistemas de alicerçamento da Segurança Pública, qual seja, a normativa penal, manifestou incapacidade operativa frente ao dilema posto, é justificável a mitigação do direito à inovação até que se tenha substrato penal apto para responder aos desdobramentos dos acontecimentos desencadeados por veículos autônomos. Portanto, para que não seja prestigiada a *dissimulação de condições* internas para recebimento dessa nova tecnologia, deverão os legisladores e operadores do direito se aproximarem dos conteúdos socio-criminais que se desdobram da ponderação exercida entre os dois

²⁹ Lembre que a responsabilização nos casos de omissão do garante, bem como no uso desvirtuado da "coisa", já se resolvem pelos axiomas da imputabilidade penal.

direitos constitucionalmente previstos, a fim de que não *baste* a simples "civilização" de conteúdos penais empiricamente constatados.

Reconhecida, então, a necessária *intromissão* do direito ao campo da inovação tecnológica automatizada (ao menos no que diga respeito à seara de cunho criminal) como meio legítimo a propor uma solução sincrética - desde que respeitadas as premissas aportadas para regulação do caso paradigma. Pode-se partir da irrestrita proibição destes mecanismos no sistema viário brasileiro³⁰ à cegueira deliberada institucional, que debilmente se centrará sobre a tópica em nome dos mandamentos - de cunho *aparentemente progressivo* - da inovação. No entanto, o que aqui se sugere é a adoção de medidas qualitativamente equilibradas para que esses autômatos possam entrar em circulação e, para tal, devem ser observadas as demandas e possibilidades do sistema nacional antes dessa incorporação.

A partir daí, algumas são as alternativas *viáveis* para atender às súplicas do sistema de Segurança Pública, embora todas advenham do reconhecimento da necessidade de imposição regulatória estatal³¹. É possível, por exemplo, cogitar a responsabilidade penal da pessoa jurídica responsável pelo produto (máquina autônoma) (SHECAIRA, 2011) - prescindindo-se da análise de culpabilidade ao reconhecer a responsabilidade objetiva da empresa -, mesmo que só haja esse entendimento, no Brasil, nos casos de crimes ambientais (art. 225, §3º da Constituição Federal). Ou ainda, pormenorizar, no código penal - a dizer, no campo dos crimes previstos no Código de Trânsito Brasileiro - as situações ensejadoras de responsabilização criminal (o que poderia ser inócuo graças à natureza do mecanismo em questão). Fato é que não podemos consentir com o enfraquecimento do nosso já desgastado (e desacreditado) Sistema de Segurança, devendo o aparato estatal se mobilizar frente à nova situação de vulneração humana derivada de aportes das ciências instrumentais.

³⁰ O que provavelmente não ocorrerá, pois já há mobilização estatal para a regulamentação dos veículos autônomos no sistema viário brasileiro - vide a Portaria 2.663/2020.

³¹ Observados os ditames já trazidos na "IEEE *Ontological Standard for Ethically Driven Robotics and Automation Systems*" (IEEE 7007/2021) e na "IEEE *Standard for Transparency of Autonomous Systems*" (IEEE 7001/2021). Disponíveis em: <<https://ieeexplore.ieee.org/document/9611206>> e <<https://ieeexplore.ieee.org/document/9726144>>.

CONCLUSÃO

Com este ensaio, pretende-se lançar foco a um problema multifatorial, multisetorial e desfragmentado: a tecnologia enquanto novo f(ator) social-jurídico de risco aos direitos tutelados pelo direito penal. Objetiva-se compor uma investigação inicial acerca dos juízos de ponderação aplicáveis aos casos que contenham ou manipulem conteúdo jurídico-criminal. Objetiva-se aquecer as discussões sobre a interação homem-máquina, no campo da responsabilidade penal, tomando-se como base um objeto delimitado (qual seja, a inteligência artificial e autonomia das máquinas em confronto com a segurança social) subsidiado por aspectos sociológicos de interpretação de atos desencadeados por este binômio. A investigação teórica, permite que o caso destacado traga os resultados iniciais. Pois é a partir dele que se pode remontar à análise do risco jurídico-social das inteligências artificiais (e dirigir-se, enfim, à teoria do incremento do risco), sem necessariamente ser identificado um "ser" robô ou humano à responsabilização. Vindo a, portanto, impor delimitações ao próprio arco de programação e a liberdade de inovar, por meio do *aceite* da regulação estatal.

O risco é inerente à sociedade, eliminá-los por completo significa paralisar o desenvolvimento social e o aperfeiçoamento de novas práticas, porém há casos em que o excesso de risco incutido em determinada operação justifica a pró-atividade jurídica. Se a programação deste veículo atenta ao pacto até então firmado no tecido social (tomando para si a decisão e institucionalização de um dilema moral), abrindo caminhos a uma nova conflitualidade, é dever do Estado incorporar a complexidade criminal do caso para decidir como irá atuar. Valendo-se da autopoiese tratada por Niklas Luhmann, o sistema social, como co-criador do sistema jurídico-regulador, requisita certo grau de maleabilidade deste último, o qual se conformará (ou *não*) a partir da sua intolerância às ebulições sociais. Para se dirigir às conclusões finais do trabalho, é preciso questionar: este é um caso a suscitar adaptação sistêmica ou será apenas mais um dissabor a ser enfrentado pela população em geral? Qual a liberdade de inovar?

REFERÊNCIAS

ANTÓN, Tomás S. Vives. **Fundamentos del sistema penal**. 2. ed. Valência: Tirant lo Blanch, 2011.

BRASIL. **Constituição (1988)**. Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal: Centro Gráfico, 1988.

BECK, Ulrich. **Sociedade de risco**: rumo a uma outra modernidade; tradução de Sebastião Nascimento - 2. ed. São Paulo: Editora 34, 2011.

BUOLAMWINI, Joy; GEBRU, Timnit. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. In: **Conference on fairness, accountability and transparency**. PMLR, 2018.

BUSATO, Paulo César. **Direito penal**: parte geral, 2. ed. São Paulo: Atlas, 2013.

CICUREL, R.; NICOLELIS, M. A. L. **O cérebro relativístico**: como ele funciona e por que ele não pode ser simulado por uma máquina de Turing. 1 ed. São Paulo: Kios Press, 2015.

CORMEN, Thomas H. **Algorithms Unlocked**. MIT Press, 2013.

DENNINGER. Erhard. **Der Gebändugte Leviathan**. Baden-Baden: Nomos, 1990.

DOS SANTOS, José Vicente Tavares. **Violências e conflitualidades**. Porto Alegre, 2009, (3ª Edição), 176p.

FRAZÃO, Ana; MULHOLLAND, Caitlin (Coord.). **Inteligência artificial e direito – Ética, regulação e responsabilidade**. São Paulo: Revista dos Tribunais, 2019, p. 6.

GUEDES, Marcelo Santiago. **Veículos autônomos inteligentes e a responsabilidade civil nos acidentes de trânsito no Brasil**: desafios regulatórios e propostas de solução e regulação. Série Pesquisas ESMPU, v. 2. Brasília: ESMPU, 2020, 139p.

HABERMAS, Jurgen. **O futuro da Natureza Humana**: a caminho de uma eugenia liberal? São Paulo: Martins Fontes, 2004.

HIDALGO, César. **How humans judge machines**. Cambridge: MIT Press, 2021.

KNIGHT, W. (2018, 25 de março). **The Dark Secret at the Heart of AI**. MIT Technology Review. Artificial Intelligence/Machine Learning. Disponível em: <<https://www.technologyreview.com/s/604087/the-dark-secret-at-the-heart-of-ai/>> Acesso em: 09 nov. 2022.

LUDWIG, C. L. **A razão comunicativa e o Direito em Habermas**. Revista Direito em Debate, [S. l.], v. 7, n. 11, 2013. DOI: 10.21527/2176-6622.1998.11.%p. Disponível em: <<https://www.revistas.unijui.edu.br/index.php/revistadireitoemdebate/article/view/827>>. Acesso em: 31 out. 2022.

MELLO, Rogério Luís Marques de; LAZARI, Rafael José Nadim de. **Quem é o culpado? Uma análise criminal das interações humanas com a inteligência artificial**. Revista Brasileira de Direitos Fundamentais & Justiça, [S. l.], v. 16, n. 46, p. 123–153, 2022. DOI: 10.30899/dfj.v16i46.1116.

MENDES, Laura; MATTIUZZO, Marcela. Discriminação Algorítmica: Conceito, Fundamento Legal e Tipologia. **RDU**, Porto Alegre, Volume 16, n. 90, 2019, 39-64, nov-dez 2019.

O'NEIL, Cathy. **Weapons of math destruction: how big data increases inequality and threatens democracy**. Nova York: Crown Publishers. 2016. Edição digital.
ORDEIG, Enrique Gimbernat. **Imputação Objetiva no Direito Penal**; organização, traduções e apresentação de Pablo Rodrigo Alflen - Porto Alegre: CDS Editora, 2019. 256p.

PASQUALE, Frank. **The black box society**. The secret algorithms that control money and information. Cambridge: Harvard University Press, 2015.

RODRIGUES, Lucas de Faria. **A Concretização da Constituição Tecnocientífica: o regime jurídico fundamental da ciência, tecnologia e inovação**. Porto Alegre, RS: Editora Fundação Fênix, 2021.

ROBERTO, Enrico. **Responsabilidade civil pelo uso de sistemas de inteligência artificial: em busca de um novo paradigma**. Revista Internet e Sociedade. nº1, vº1, 2021, p. 121-143.

SARLET, Wolfgang. **A eficácia dos direitos fundamentais: uma teoria geral dos direitos fundamentais na perspectiva constitucional**. 13ª ed, Porto Alegre: Livraria do Advogado, 2018.

SHECAIRA, Sérgio Salomão. **Responsabilidade penal da pessoa jurídica**. Rio de Janeiro: Elsevier, 2011.

TEIXEIRA NETO, João Alves. **Aproximações entre direito penal e filosofia: ensaios e conferências**. Porto Alegre: livraria do Advogado, 2021.

10. TELETRIAGEM NA TELESSAÚDE (TELEMEDICINA E TELEENFERMAGEM) POR INTELIGÊNCIA ARTIFICIAL: UM OLHAR PARA OS MARCOS REGULATÓRIOS NO BRASIL

TELESCREENING IN TELEHEALTH (TELEMEDICINE AND TELENURSING) BY ARTIFICIAL INTELLIGENCE: A LOOK AT THE REGULATORY FRAMEWORKS IN BRAZIL



<https://doi.org/10.36592/9786554600552-10>

*Regina Linden Ruaro*¹

*Helen Lentz Ribeiro Bernasiuk*²

RESUMO

No presente artigo, aborda-se o tema da teletriagem realizada por inteligência artificial no sistema de telemedicina e telenfermagem, analisando os marcos regulatórios existentes no Brasil. O objetivo geral deste estudo é analisar a necessidade de regulamentação, em nível nacional, no tocante ao uso de sistemas de IA para triagem em telessaúde, no contexto da Telemedicina e Telenfermagem no Brasil; os objetivos específicos, por sua vez, desdobram-se em: (a) compreender a aplicabilidade de inteligência artificial à triagem em telemedicina; (b) verificar marcos regulatórios da telemedicina e telenfermagem no Brasil; (c) analisar necessidades de regulamentação, em nível nacional, no tocante ao uso de sistemas de IA para triagem

¹ Doutora em Direito pela Universidad Complutense de Madrid (1993) com título revalidado pela UFRGS. Pós-doutorado pela Universidad San Pablo - CEU de Madri (2006/2008). Estágio Pós-doutoral na Universidade San Pablo - CEU de Madri (2016). Compõe o Grupo Internacional de Pesquisa " Protección de Datos, Transparencia y Acceso a la Información". Advogada e Consultora jurídica nas áreas do Direito Administrativo, Direito Digital e da Proteção de Dados Pessoais. Professora Titular da Escola de Direito da PUCRS. Procuradora Federal/AGU (aposentada). Professora convidada do Máster en Protección de Datos, Transparencia y Acceso a la Información da Universidad San Pablo de Madrid-CEU/ Espanha. Decana Associada da Escola de Direito da PUCRS (2018/2021). Membro do Comitê Gestor do Biobanco da PUCRS. Membro Honorário do Instituto Internacional de Estudos de Direito do Estado - IEDE. Lidera o Grupo de Pesquisa cadastrado no CNPq: Proteção de Dados Pessoais e Direito Fundamental de Acesso à Informação no Estado Democrático de Direito na linha de Tecnologia, Direito e Inovação na PUCRS. E-mail: regina@ruaro.adv.br

² Doutoranda em Direito pela PUCRS. Mestre em Direito pela PUCRS. Especialista em Direito Civil pela UFRGS. Especialista em Direito Público pela Uniderp. Diritto Costituzionale Comparato e Cultura Giuridica Europea pela Sapienza, Università di Roma. (Roma- Itália). La constitución del algoritmo: Inteligencia artificial y Derecho, Universidad de Granada (Granada- Espanha). Bolsista Capes/Proex PPGD/PUCRS. Advogada. <http://lattes.cnpq.br/4798723812833494>. Código Orcid: <https://orcid.org/0000-0002-6224-1251>. E-mail: helenbernasiuk@gmail.com.

em telemedicina por planos de saúde privados e Sistema Único de Saúde – SUS. O estudo se caracteriza pelos métodos indutivo e dialético. O tema da inteligência artificial, bem como da telemedicina e uso de robô para teletriagem já são objeto de estudo em áreas que dialogam com o Direito, tais como a medicina e tecnologia. Ademais, o primeiro é matéria de Projeto de Lei em tramitação (PL 21/20). O método exploratório, sob o viés qualitativo, apresenta-se como via para subsidiar reflexões e conclusões, ainda que provisórias, sobre uma demanda social por saúde e as recentemente aprovadas resoluções que dispõem sobre a telemedicina e telenfermagem no que tange à teletriagem via IA. Procede-se, neste recorte de estudo, às técnicas de pesquisa bibliográfica e documental, pelas quais se buscam leis, normativas e orientações sobre o tema. A interpretação dos dados se dá via método sociológico, uma vez que o tema refere-se ao direito à saúde, inovações e tendências tecnológicas e as áreas da medicina e enfermagem. Ressalta-se que o presente artigo integra a linha de pesquisa *Direito, Ciência, Tecnologia & Inovação*, do Programa de Pós-Graduação em Direito da Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS).

Palavras-chave: Teletriagem; Telemedicina; Telessaúde; Inteligência Artificial; Marcos regulatórios no Brasil.

ABSTRACT

This article addresses the issue of telescreening carried out by artificial intelligence in the telemedicine and telenursing system, analyzing the existing regulatory frameworks in Brazil. The general objective of this study is to analyze the need for regulation, at the national level, regarding the use of AI systems for triage in telehealth, in the context of Telemedicine and Telenursing in Brazil; the specific objectives, in turn, unfold into: (a) understanding the applicability of artificial intelligence to telemedicine triage; (b) verify regulatory frameworks for telemedicine and telenursing in Brazil; (c) analyze regulatory needs, at the national level, regarding the use of AI systems for triage in telemedicine by private health plans and the Unified Health System – SUS. The study is characterized by inductive and dialectical methods. The theme of artificial intelligence, as well as telemedicine and the use of robots for telescreening, are already being studied in areas that dialogue with Law,

such as medicine and technology. In addition, the first is the subject of a bill in progress (PL 21/20). The exploratory method, under the qualitative bias, is presented as a way to support reflections and conclusions, albeit provisional, about a social demand for health and the recently approved resolutions that provide for telemedicine and telenursing with regard to telescreening via AI. In this part of the study, bibliographical and documental research techniques are used, through which laws, regulations and guidelines on the subject are sought. The interpretation of the data is carried out via the sociological method, since the theme refers to the right to health, innovations and technological trends and the areas of medicine and nursing. It should be noted that this article is part of the Law, Science, Technology & Innovation research line of the Graduate Program in Law at the Pontifical Catholic University of Rio Grande do Sul (PUCRS).

Keywords: Telescreening; Telemedicine; Telehealth; Artificial intelligence; Regulatory frameworks in Brazil.

1 INTRODUÇÃO

A pandemia de Sars-Cov-2, causadora de uma das maiores crises de saúde pública a nível global conhecidas pela humanidade, acelerou a busca por estratégias para lidar-se com o problema causado pelo lockdown, pela impossibilidade de que as consultas médicas se dessem na forma presencial. Buscando forma de resolver-se o problema é que no Brasil foram regulamentados os atendimentos médicos à distância através da Lei n. 13.989, de 15 de abril de 2020, que autorizou o uso de telemedicina durante a fase crítica da Covid-19 (BRASIL, 2020). A mesma lei determinava que, transcorrido o período crítico, caberia ao Conselho Federal de Medicina – CFM dispor sobre a regulamentação dessa modalidade de atendimento médico.

A matéria evoluiu e a regulamentação passou a dar-se através da Lei n. 14.510, de 27 de dezembro de 2022³(BRASIL, 2022) que alterou a Lei n. 8.080, de 19

³ A Lei n. 14.510, altera a Lei nº 8.080, de 19 de setembro de 1990, para autorizar e disciplinar a prática da telessaúde em todo o território nacional, e a Lei nº 13.146, de 6 de julho de 2015; e revoga a Lei nº 13.989, de 15 de abril de 2020.

de setembro de 1990 autorizando e disciplinando a prática de telessaúde em todo o território nacional. Neste sentido, o art. 26- A, dispõe que a telessaúde abrange “a prestação remota de serviços relacionados a todas as profissões da área da saúde regulamentadas pelos órgãos competentes do Poder Executivo federal”.⁴ (BRASIL, 2022).

Na esteira de avanços regulatórios e tecnológicos legados da pandemia, assiste-se a um fenômeno de mercado alavancado pela necessidade de resposta rápida imposta pelo cenário de crise de saúde coletiva. Note-se que a telemedicina, é um setor que deve movimentar mais de U\$ 130 bilhões até 2025 e a tendência é de aumento contínuo por demandas de pacientes nessa modalidade, incentivo a médicos e operadoras de saúde, bem como uma escalada de implementação de sistemas de inteligência artificial (CABRINI, 2022). O uso de inteligência artificial (doravante utilizaremos a sigla IA), nesse sentido, pode ser um aliado da garantia à saúde, direito básico de cidadãos e cidadãs brasileiros consoante a Constituição Federal de 1988 (BRASIL, 1988). Urge, portanto, que a legislação brasileira e órgãos regulatórios acompanhem tais avanços. Do mesmo modo, é imprescindível estudar o assunto no âmbito do Direito.

Assim, como problema de pesquisa do presente artigo questiona-se: há bases legais, no Brasil, para implementação de sistemas de IA em teletriagem de pacientes? Tal abordagem se justifica, ainda, pela verificação de que tecnologias do tipo já são uma realidade no país.

O objetivo geral deste estudo é analisar a necessidade de regulamentação, em nível nacional, no tocante ao uso de sistemas de IA para triagem em telessaúde, no contexto da Telemedicina e Telenfermagem no Brasil. Já os objetivos específicos desdobram-se em: (a) compreender a aplicabilidade de inteligência artificial à triagem em telemedicina; (b) verificar marcos regulatórios da telemedicina e telenfermagem no Brasil; (c) analisar necessidades de regulamentação, em nível nacional, no tocante ao uso de sistemas de IA para triagem em telemedicina por planos de saúde privados e Sistema Único de Saúde – SUS.

⁴ A Lei n. 14.510, altera a Lei nº 8.080, de 19 de setembro de 1990, para autorizar e disciplinar a prática da telessaúde em todo o território nacional, e a Lei nº 13.146, de 6 de julho de 2015; e revoga a Lei nº 13.989, de 15 de abril de 2020.

Este estudo se caracteriza pelos métodos indutivo e dialético. O tema da inteligência artificial, bem como da telemedicina e uso de robô para teletriagem já são objeto de estudo em áreas que dialogam com o direito, tais como a medicina e tecnologia. Ademais, o primeiro é matéria de Projeto de Lei N. 21/20– PL em tramitação. O método exploratório, sob o viés qualitativo, apresenta-se como via para subsidiar reflexões e conclusões, ainda que provisórias, sobre uma demanda social por saúde e as recentemente aprovadas resoluções que dispõem sobre a telemedicina e telenfermagem no que tange à teletriagem via IA. Procede-se, neste recorte de estudo, às técnicas de pesquisa bibliográfica e documental, pelas quais se buscam leis, normativas e orientações sobre o tema. A interpretação dos dados se dá via método sociológico, uma vez que o tema refere-se ao direito à saúde, inovações e tendências tecnológicas e as áreas da medicina e enfermagem (FINCATO; GILLET, 2018).

Este artigo divide-se em duas seções principais: na primeira, faz-se uma revisão sobre os conceitos de triagem, inteligência artificial e a aplicação desta última à área da saúde. Toma-se como referência, sobretudo, artigos que tratam do assunto. Já na segunda seção, adentra-se no foco investigativo, qual seja, a regulamentação e legislação nacional acerca de teletriagem em saúde, atendimento em saúde mediado por tecnologias computacionais e, especificamente, no que se refere ao desenvolvim e uso de IA's no Brasil em contextos gerais. Nessa seção, são estabelecidas, ainda, relações com o tema e a LGPD, bem como no que tange à Constituição Federal. As considerações finais, por sua vez, retomam os objetivos e problema de pesquisa aqui propostos, oferecendo, por fim, percepções oriundas da investigação.

2.1. A TRIAGEM EM SAÚDE EM AMBIENTES DE SAÚDE TRADICIONAL

Para que se possa adentrar ao tema objeto do presente artigo, é importante, ainda que de forma breve, apresentar-se os conceitos pertinentes aos temas da triagem e como ela se dá em ambientes de saúde tradicionais. De modo que se estabeleça uma linha de reflexões de forma sequencial: triagem em saúde, IA e suas

aplicações na saúde, bem como os usos desses sistemas no campo da saúde no contexto contemporâneo. Chega-se, ao fim do capítulo ao tema da teletriagem.

Triagem é um termo amplo e, em um espaço de saúde, diversas categorias profissionais participam, de certo modo, desse processo, ainda que não sejam médicos ou enfermeiros. Ou seja, mesmo o setor administrativo ou recepcionistas exercem o papel de ouvir as demandas do paciente e auxiliá-lo no encaminhamento para a próxima etapa do percurso até a equipe de enfermagem e médica em suas diferentes especialidades e níveis de urgência. Cabe, no entanto, a equipes de medicina e enfermagem a análise e registro de sintomas, aferição de parâmetros clínicos e classificação de riscos para o devido atendimento (GIGLIO-JACQUEMOT, 2005).

Em artigo caracterizado como revisão integrativa de produções científicas acerca das funções do profissional de enfermagem no contexto de triagem, Acosta, Duro e Lima (2012) citam um aumento de procura, em nível mundial, por serviços de urgência. Conforme os autores, a triagem cumpre o papel de organizar os graus de emergência e, então, priorizar os atendimentos. Ainda segundo os referidos pesquisadores, há distinções entre as funções e protocolos em relação aos profissionais que os executam, a depender também do contexto de atendimento. Nesse sentido, esclarecem que, no Brasil, a triagem feita por enfermeiras e enfermeiros é estruturada sobre a Política Nacional de Humanização – PNH, que preconiza uma etapa de acolhimento ao paciente. Esses profissionais devem, assim, afastar práticas de exclusão de pessoas, ampliar o acesso à rede de saúde, além de oferecer “atendimento acolhedor e resolutivo” (p. 182).

Na etapa de triagem, consta a classificação de risco do paciente que busca atendimento em saúde. Trata-se, possivelmente, de uma das funções mais conhecidas da triagem pela sociedade, uma vez que as categorias de risco são pré-definidas e seguem protocolo padronizado. Nesse sentido, os resultados do citado estudo apontaram essa característica como uma das atividades preponderantes de equipes de enfermagem:

Em relação às atividades desenvolvidas pelo enfermeiro na triagem/classificação de risco, os estudos destacaram a avaliação do usuário e

tomada de decisão, determinando a classificação e priorização do atendimento no serviço de urgência de acordo com a gravidade. O enfermeiro possui conhecimentos e habilidades específicos para definição da prioridade de atendimento, que correspondem desde o conhecimento administrativo e clínico e olhar usuário, até as habilidades de intuição e comunicação. Assim, o enfermeiro administra o fluxo de oferta e demanda dos usuários nos serviços de urgência do serviço, contribuindo para a diminuição da morbi- -mortalidade (ACOSTA; DURO; LIMA, 2012, p. 188).

Complementa-se as considerações supraexpostas com achados de estudo realizado uma década depois. Nesse sentido, em artigo de revisão sistemática que versa sobre a efetividade de usos de protocolos avançados de triagem, Soster *et al.* (2022) mensuraram, via metanálise de ensaios clínicos randomizados, questões como tempo de permanência, segurança e satisfação dos sujeitos, profissionais e pacientes, quanto aos protocolos brasileiros. Assim como Acosta, Duro e Lima (2012) apontam, Soster *et al.* (2022) também citam o crescimento exponencial, registrado desde os anos 1990, das buscas por atendimento em saúde. Eles também referem as superlotações dos serviços em nível mundial e a busca, empreendida sobretudo por gestores, por desafogar o sistema de saúde.

Os referidos autores esclarecem que o sistema de triagem por classificação de risco, implementado na última década do século XX na Europa, afigurava-se como promissor. Esses protocolos, no entanto, adotados amplamente por demais países nos anos 2000, não se mostraram eficazes. A partir disso, passaram a ser implementados protocolos de triagem avançada, via pela qual os profissionais de enfermagem já iniciam procedimentos de atendimento antes mesmo de o paciente ser atendidos por equipes médicas. Tal prática passou, então, a ser vista como potencialmente capaz de reduzir custos e, concomitantemente, diminuir tempo de espera por atendimento, bem como aumentar a satisfação dos sujeitos envolvidos.

Os pesquisadores, acima referidos, verificaram que a redução média em tempo de espera alcança 36 minutos. Além disso, concluíram que “Os profissionais de triagem são competentes para iniciar condutas diagnósticas na triagem de forma segura, desde que treinados para tal, e estas medidas refletem um aumento na

satisfação dos pacientes” (SOSTER *et al.*, 2022, p. 9). Apesar de os resultados sugerirem diminuição de custos aos serviços de saúde, os autores indicam, por fim, a necessidade de mais estudos sobre as relações entre o impacto econômico e protocolos de triagem avançada.

Pelos estudos apontados, percebe-se que as atividades de triagem em saúde são executadas, no Brasil, classicamente por profissionais da enfermagem, e não se restringem aos serviços de emergência. Evidencia-se, ademais, que a prática exige níveis de segurança para a correta destinação de pacientes que buscam atendimento. Nota-se, além disso, que um problema que se impõe é o da superlotação e a necessidade de redução de custos. Assim sendo, recursos tecnológicos apresentam-se, *a priori*, como um caminho a ser considerado e neste aspecto, a importância do uso da inteligência artificial.

2.2. O USO DA INTELIGÊNCIA ARTIFICIAL NA TELESSAÚDE

Antes de mais nada, salienta-se que o conceito de Inteligência Artificial não é pacífico (FREITAS; FREITAS, 2020, p. 27). No entanto, como a discussão conceitual não é objeto do presente estudo, adota-se como definição a de que aquela é compreendida como um sistema que, a partir de máquinas, realiza previsões, recomendações e decisões conforme objetivos definidos em seu código. É capaz, assim, de operar com vários níveis de autonomia e, em muitos casos, definir ações que prescindem da análise humana. Trata-se, desse modo, de tecnologias avançadas que tornam máquinas capazes de compreender, aprender e tomar decisões em nível similar às capacidades humanas (RUARO; REIS, 2020).

No Brasil, cumpre assinalar a existência da Estratégia Brasileira de Inteligência Artificial, a qual possui como objetivo elaborar um plano para o desenvolvimento de estratégias acerca de Inteligência Artificial e a disseminar o uso consciente e ético desses sistemas. Segundo o relatório, um dos seguimentos com maior exponencial de crescimento de inteligência artificial é a área da saúde, na parte de diagnósticos e tratamentos de saúde (EBIA, 2021).⁵

⁵ Instituída pela Portaria MCTI nº 4.617, de 6 de abril de 2021, alterada pela Portaria MCTI nº 4.979, de 13 de julho de 2021 (Anexo). BRASIL, Ministério da Ciência, Tecnologia e Inovações. **Estratégia**

No Congresso Nacional, o projeto mais relevante acerca da temática é o n. 21/20, que estabelece diretrizes para a utilização de Inteligência Artificial e, conceitua o termo inteligência artificial como sendo um sistema baseado em processo computacional que, "a partir de um conjunto de objetivos definidos por humanos, pode, por meio do processamento de dados e de informações, aprender a perceber e a interpretar o ambiente externo, bem como a interagir com ele, fazendo previsões, recomendações, classificações ou decisões (BRASIL, 2020)"⁶.

Segundo João de Fernandes Teixeira, para que seja considerada uma inteligência artificial "é preciso que essa máquina imite nossa atividade mental quando estamos fazendo uma operação aritmética" (TEIXEIRA, 2017, p.16).

Em face da utilização massiva de IA no cotidiano é possível afirmar que é uma das tecnologias mais importantes do século XXI (COMISSÃO EUROPEIA, 2018). Consoante investigação de Nunes, Guimarães e Dadalto (2022), há uma crescente demanda de uso de IA em sistemas de saúde. Segundo eles, medidas inteligentes em saúde pública, no entanto, datam do século XIX, quando se passou a adotar medidas de saneamento – a chamada era 1.0 da saúde. Já no século XX, na era 2.0, a característica principal foi a ampliação da indústria farmacêutica, que, a partir da adoção de tecnologias industriais, propiciou a produção em larga escala de medicamentos como antibióticos. A era 3.0 iniciou-se nos anos 1980, adentrando, então, na adoção de tecnologias computacionais. Exames de imagem e acesso, via internet, à literatura médica são os avanços citados pelos autores como propulsores de melhorias na área da saúde. Quanto ao presente, esclarecem:

Atualmente, o mundo vive a era de cuidados de saúde 4.0, caracterizada pela medicina inteligente. Acompanhando a nova onda de revolução tecnológica, essa fase é dominada em grande parte por IA, automação, big data, medicina de precisão, telemedicina etc., sendo reconhecida como a era em que a medicina ganhou novo cérebro e novas mãos. Assim, notícias de uso da IA no campo da

Brasileira de Inteligência Artificial – EBIA. Disponível em: <https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/inteligencia-artificial>. Acesso em: 05 fev. 2023.

⁶ Existem outros projetos, mas o mais significativo é o nº21/20. Conforme se verifica no art. 2º do **Projeto de Lei n. 21/2020**. Estabelece fundamentos, princípios e diretrizes para o desenvolvimento e a aplicação da inteligência artificial no Brasil; e dá outras providências. Brasília: Senado Federal, 2020. Disponível em: <https://www.camara.leg.br/propostas-legislativas/2236340>. Acesso em: 05 fev. 2023.

saúde são frequentes, e sua utilização para prevenir, detectar e tratar doenças vem sendo largamente pesquisada (NUNES; GUIMARÃES; DADALTO, 2022, p. 84).

Lobo (2017) introduz o tema da aplicação de IA à área da saúde ao citar os diversos usos que esses recursos tecnológicos oferecem: analisar grandes volumes de dados para propor soluções a problemas médicos; armazenar, recuperar e verificar exames para gerar probabilidades de diagnóstico; acompanhar evolução de enfermidades, entre outros. O autor destaca, ainda, o uso de *wearable devices*, dispositivos que, conectados ao corpo humano, são capazes de aferir diversos parâmetros médicos e, então, tomar decisões como injetar insulina (no caso de diabéticos) e/ou outros procedimentos. Ele cita, ademais, que a "adoção de sistemas de apoio à decisão clínica para melhorar a acurácia da medicina, considerando o aumento da carga de trabalho de médicos em emergências e clínicas de família" pode ser benéfica (LOBO, 2017, p. 187). Nesse sentido, complementa:

Em 2009, verificou-se que 32% dos erros médicos nos EUA resultavam da diminuição do tempo de interação do médico com os pacientes, produzindo diagnósticos equivocados, não reconhecimento da urgência ou piora da evolução do paciente que demandariam prescrever ou realizar ações pertinentes. Mesmo em hospitais que disponham de prontuários médicos eletrônicos⁷, com a possibilidade de melhor coleta de dados, admite-se que 78,9% dos erros médicos estariam relacionados a problemas na relação médico-paciente, exame clínico deficiente, falha de avaliação dos dados do paciente ou falta de exames que comprovassem a hipótese diagnóstica (LOBO, 2017, p. 187).

O autor conclui, no estudo citado, que a adoção de sistemas de IA na área da saúde tende a aumentar e salienta que se trata de uma realidade já consolidada em diversos países. Outrossim, analisa que o aperfeiçoamento dessas tecnologias, o que se dá, inclusive, pelas próprias capacidades de os sistemas aprenderem, tem potencial para prevenir e tratar complicações de saúde. Isso, no entanto, assevera, deve estar atrelado a práticas humanas, ou seja, em sua visão, a relação entre profissional de saúde e paciente, bem como a tomada de decisões em conjunto segue indispensável.

Em outro texto, ele questiona, contudo, como tal grau de atenção poderia ser aplicável ao Sistema Único de Saúde – SUS brasileiro, cujo tempo que os médicos conseguem dedicar ao paciente é escasso (LOBO, 2018). Nesse contexto, defende que práticas em saúde podem se beneficiar com uma integração com sistemas de IA, em ações como registro de dados em prontuários, acompanhamento de pacientes via telemedicina, sistemas de apoio às decisões clínicas, entre outros. Destaca-se, ademais, este item referido pelo pesquisador: “Emprego de sistemas de apoio à decisão clínica orientando, a partir dos sintomas e sinais apresentados pelo paciente, hipóteses de diagnóstico, exames e tratamentos a serem prescritos” (LOBO, 2018, p. 6).

Além de confirmar tendências já observadas por estudiosos que se dedicam às imbricações entre IA e saúde, a chegada da Covid-19 acelerou a adoção desses recursos tecnológicos. Acerca do uso de IA no contexto da pandemia, destaca-se um dos recursos que se mostrou eficaz para auxiliar profissionais e pacientes na detecção da doença. Vale lembrar que, sobretudo na fase inicial da propagação do vírus causador da enfermidade, o cenário caótico complicava-se diante das dificuldades diagnósticas, com escassez de testes e o incipiente conhecimento científico sobre o assunto. Nesse sentido, acrescenta-se:

Com a pandemia de covid-19, a utilização da IA na área de saúde se tornou ainda mais comum. Estudo publicado em março de 2020 na revista *Radiology* afirma que a IA de aprendizagem profunda pôde detectar covid-19 com precisão a partir de imagens de tomografia computadorizada (TC) de tórax, e distingui-la de pneumonia e outras doenças, pulmonares ou não. Com isso, a detecção da doença torna-se mais célere, visto que a TC de tórax poderia ser usada como abordagem rápida e confiável para o rastreamento da covid-19 (NUNES; GUIMARÃES; DADALTO, 2022, p. 85).

Já no Brasil, no primeiro ano de pandemia, iniciaram-se estudos com o robô Laura Care, cujos resultados preliminares se mostraram promissores, uma vez que a medida se provou eficaz para auxiliar a desafogar o sistema de saúde naquele momento de crise. O robô, que funcionou como triagem de pacientes, foi capaz de

identificar, entre 24,1 mil pessoas, que 44,8% dos casos apresentavam sintomas leves de Covid-19, auxiliando na gestão de atendimento (MORALES *et al.*, 2021).

Os estudos revisados para o desenvolvimento deste artigo convergem quanto ao entendimento de que a adoção de IA na área da saúde é cenário posto. Restou evidenciado que tal conjectura foi acelerada pela crise sanitária iniciada em 2020 e os potenciais benefícios dessas tecnologias nos campos do atendimento em saúde são inegáveis, o que se estende ao tema da teletriagem. Salienta-se, no entanto, que esse emprego precisa ser concatenado com demais demandas sociais, especialmente no que se refere à sua segurança. Isso, entende-se, passa por uma regulamentação clara, adequada e capaz de acompanhar o contexto contemporâneo. A próxima seção deste estudo, então, avança para o campo do direito, o que se dá via análise do arcabouço regulatório e legislativo sobre o assunto.

3 LEGISLAÇÃO E TELETRIAGEM EM SAÚDE: A REALIDADE BRASILEIRA

A fim de adentrar nas questões pertinentes à saúde e tecnologia, especialmente no que se refere à teletriagem, cumpre destacar que, em maio de 2022, o CFM publicou a Resolução n. 2.314. O documento definiu modalidades das interações entre médicos e pacientes mediadas por tecnologias de comunicação e criou um marco regulatório para o tema. Ressalta-se, assim, que o termo telessaúde, conforme define o órgão regulador, é amplo e engloba uma gama de serviços e profissionais de saúde no contexto das tecnologias digitais; telemedicina, por seu turno, restringe-se aos atos e procedimentos médicos realizados por esta categoria profissional. Já em seu art. 5º, o referido documento estabelece que os teleatendimentos em telemedicina podem ser exercidos nas modalidades de consulta, diagnóstico, monitoramento, vigilância e, enfatiza-se, teletriagem, entre outros (CONSELHO FEDERAL DE MEDICINA, 2022).

No mesmo período, o Conselho Federal de Enfermagem – COFEN dispôs sobre o tema, via Resolução n. 696, que normatiza o exercício de telenfermagem nos âmbitos do SUS, saúde suplementar e privada. Em seu art. 2º, o documento define que ta prática abrange: “Consulta de Enfermagem, Interconsulta, Consultoria, Monitoramento, Educação em Saúde e Acolhimento da Demanda Espontânea

mediadas por Tecnologia da Informação e Comunicação (TIC)". Frise-se, ainda, que "A prática de Enfermagem mediada por TIC deverá prescindir de registro ativo junto ao Conselho Regional de Enfermagem" (CONSELHO FEDERAL DE ENFERMAGEM, 2022).

A teletriagem médica, assunto deste trabalho, é definida no art. 11 da Resolução 2.314 como ato realizado por médico com vistas ao direcionamento do paciente à assistência que melhor julgar necessária ao caso relatado e/ou regulação ambulatorial ou hospitalar. Ademais, o documento define que o médico deverá destacar, ao paciente, que seu parecer é uma "impressão diagnóstica de gravidade" e que o sistema ou estabelecimento de saúde "deve oferecer e garantir todo o sistema de regulação para encaminhamento dos pacientes sob sua responsabilidade" (CONSELHO FEDERAL DE MEDICINA, 2022).

Destaca-se, outrossim, que a referida Resolução versa acerca da relação médico-paciente e, portanto, silencia acerca do uso de tecnologias de IA no que tange à teletriagem médica. O mesmo se observa na Resolução n. 696/2022 do COFEN, que, igualmente, estabelece que o exercício de telenfermagem deve ser realizado em consonância com os seus dispostos. Estes, enfatiza-se, sequer incluem a prática de teletriagem entre as prerrogativas do profissional de enfermagem em atos mediados por tecnologias da informação e comunicação.

A legislação brasileira, a partir da edição da Lei n. 14.510, de 27 de dezembro de 2022, autoriza e disciplina a prática de telessaúde em todo o território nacional, abrangendo todas as profissões regulamentadas pelos órgãos competentes do Poder Executivo federal (BRASIL, 2022).

Sendo assim, é notório que, em contraste com os achados dos estudos revisados anteriormente, a triagem, quando mediada por tecnologias, sobrecarrega a figura do profissional de medicina. Enfatiza-se, ademais, que a modalidade de teletriagem aqui citada diz respeito a interações humanas, ou seja, implica categorias profissionais em contato com pacientes. Assim, esses regulamentos não necessariamente avançam para a temática da IA aplicada à teletriagem.

Nesse sentido, a Organização Mundial da Saúde – OMS destacou, em relatório publicado em 2021, após dois anos de consultas junto a especialistas na área, os potenciais benefícios do uso de IA em serviços de atenção à saúde. O documento,

aponta, no entanto, que tais tecnologias não devem ser superestimadas e que “seu uso não regulamentado poderia subordinar os direitos e interesses dos pacientes e das comunidades aos poderosos interesses comerciais de empresas de tecnologia ou aos interesses dos governos em vigilância e controle social”. Além disso, a entidade afirma que leis e políticas públicas, em consonância com direitos humanos, devem nortear governos, fornecedores e designers em todas as etapas do desenvolvimento e implementação de tecnologias de IA na área em saúde (ORGANIZAÇÃO PAN-AMERICANA DA SAÚDE, 2021).

Nesta seara, cita-se o Projeto de Lei n. 21/2020, ainda em tramitação, que dispõe acerca do desenvolvimento e implementação de sistemas de IA nos setores públicos e privados (BRASIL, 2020). Em linhas gerais, o referido PL propõe diretrizes abrangentes que visam ao bem-estar social, compatibilizado com o desenvolvimento econômico e o avanço tecnológico. Acentua, ademais, a centralidade do respeito à dignidade humana. Além disso, ao abordar o quesito segurança, o texto prevê que o uso de IA seja pautado em normas de gerenciamento de riscos e adoção, pelo agente desenvolvedor, de medidas que garantam o bom funcionamento do sistema. Ressalta-se, ainda, que o PL, se aprovado tal como ora se apresenta, exigirá que a implantação de um sistema de IA dê-se tão somente após avaliação sobre objetivos, benefícios e riscos, respeitando-se os dispositivos da Lei Geral de Proteção de Dados – LGPD (BRASIL, 2018).

A esse respeito, acrescenta-se a seguinte reflexão:

É necessário que haja ética em todas as etapas do desenvolvimento da IA, e esse processo é iniciado com o senso de responsabilização daqueles que programam a máquina. Eles devem preservar a integridade científica durante todo o processo, desde a coleta e manejo de dados até a divulgação dos resultados para a comunidade científica. Devem ser imparciais quanto aos resultados obtidos e possíveis danos aos usuários, incorporando o princípio bioético da não maleficência (NUNES; GUIMARÃES; DADALTO, 2022, p. 87).

A teletriagem feita por IA, nesse sentido, carece de atenção especial. Em primeiro lugar, evidentemente, no que se refere à garantia da integridade da vida

humana, haja vista que não se pode aceitar o risco de que, por erro tecnológico de qualquer natureza, a despeito do grau de avanço de tais sistemas, situações graves sejam menosprezadas. O direito à vida e à saúde, vale lembrar, é assegurado aos cidadãos e cidadãs brasileiras na Constituição Federal de 1988 e, portanto, um pilar de quaisquer iniciativas na área da saúde (BRASIL, 1988). Um segundo ponto diz respeito não apenas à Constituição, que contempla o direito à privacidade, à não-discriminação e à proteção da pessoa humana como bases da nação, mas também à própria LGPD, que se aprofunda no tema da proteção dos dados pessoais sensíveis (BRASIL, 2018).

Coleta e armazenagem de dados de saúde, nessa ordem, classificam-se como dados pessoais sensíveis e recebem tratamento especial na LGPD, justamente por seu potencial de dano aos seus titulares em casos de usos inadequados. Assim, urge considerar o risco da adoção de sistemas de IA em saúde em geral, e não apenas no que se refere à teletriagem, de forma integrada com, por exemplo, planos de saúde, indústria farmacêutica, seguradoras, empregadores, entre outros (BERNASIUK, 2021). Assim, “Diante desse parâmetro, percebe-se que a educação para uso da IA em saúde deve focar não somente o manejo da tecnologia, mas principalmente o modo de lidar com o paciente” (NUNES; GUIMARÃES; DADALTO, 2022, p. 87).

A legislação que regulamenta a telessaúde no Brasil (art. 26- A, da Lei nº14.510, de 27 de dezembro de 2022) aduz a necessidade de obediência de alguns princípios como, por exemplo: a autonomia do profissional de saúde; a necessidade do consentimento livre e informado do paciente; direito de recusa ao atendimento na modalidade telessaúde, garantido sempre o atendimento presencial quando solicitado; confidencialidade dos dados; responsabilidade digital, dentre outros (BRASIL,2022.)

Outra circunstância que carece de olhares atentos, inclusive no que tange à triagem, diz respeito a sistemas de IA projetados para uso geral, tais como a Alexa, da Amazon, e o ChatGPT, da OpenAi. Como visto anteriormente, triagem, *per si*, é um conceito amplo e pode envolver sujeitos que se propõem a auxiliar pacientes. Isso engloba categorias profissionais, com formação na área da saúde ou não (GIGLIO-JACQUEMOT, 2005). É preciso considerar, neste cenário, por exemplo, o uso de IA's cada vez mais avançadas como apoio na área da saúde, seja pelo próprio paciente,

seja por outrem ou, ainda, por sistemas legados. E esse cenário não está distante. A empresa OpenAI disponibilizou, em março de 2023, a sua *Application Programming Interface* – API, que permite integração com outros sistemas. Trata-se de uma estratégia de monetização da companhia, que passa a permitir, via pagamento, o uso da tecnologia por desenvolvedores externos (ROSA, 2023).

Isso significa que, em um futuro não tão distante, esta e outras IA's originadas em uma corrida mundial pelo desenvolvimento dessas tecnologias e, por conseguinte, domínio do mercado, possam ser integrada a incontáveis setores da saúde. Entende-se, assim, que regulamentações claras e específicas sobre tais aplicações são de salutar relevância e devem ater-se à área da saúde, com vistas a tratamento diferenciado a um tema que envolve, diretamente, a vida da população brasileira e seu direito à proteção de dados sensíveis na área em saúde.

CONCLUSÕES

Este estudo, como visto anteriormente, teve como objetivo geral analisar bases legais para desenvolvimento, implementação e uso de sistemas de inteligência artificial para triagem de pacientes no contexto de Telemedicina e Telenfermagem e suas vantagens. Assim, procedeu-se, inicialmente, a uma revisão de conceitos e estudos na área da saúde, via pela qual foi possível verificar que triagem em saúde é um termo amplo, que, em linhas gerais, diz respeito a conduzir adequadamente o paciente às etapas seguintes do atendimento. Em sentido *strictu sensu*, no Brasil, essa função é exercida sobretudo por profissionais da enfermagem, que, além de aferir parâmetros clínicos e registrá-los em prontuário, classificam o paciente conforme a urgência do quadro e, podem, ainda, realizar procedimentos anteriores ao atendimento médico.

No que tange ao objetivo específico de compreender a aplicabilidade de IA à teletriagem em saúde, verificou-se que esta área já se serve de uma série de sistemas de inteligência para auxiliar pacientes e profissionais no que tange à prevenção, monitoramento e, inclusive, aplicação de medicações. Assim, tal interface já é uma realidade no mundo e a tendência é de que sua adoção se dê, cada vez mais, em larga escala. O potencial disso é notório, uma vez que a tecnologia, desde que

sejam respeitados parâmetros bioéticos, é capaz de otimizar atendimentos em saúde, especialmente em saúde pública, ampliando o acesso a serviços por cidadãos. Nesse sentido, IA's utilizadas durante a crise sanitária causada pela Covid-19 mostraram-se promissoras.

Quanto ao objetivo específico de verificar marcos regulatórios da telemedicina e telenfermagem no Brasil, o CFM cita a teletriagem como uma das atividades em telemedicina. Entretanto, a regulamentação sobre o tema refere-se a atendimentos nos quais há interação entre médico e paciente mediada por recursos tecnológicos. O CFEN, que também tem regulamentação práticas de telenfermagem, não se refere ao tema da teletriagem. Ambos os órgãos, voltados às práticas de pessoas das categorias profissionais a eles subordinadas, não versam sobre teletriagem feita por IA. Do mesmo modo, a Lei n.14.510, de 27 de dezembro de 2022, que disciplina e autoriza a prática de telessaúde no Brasil, silencia acerca da utilização de IA. Assim, atingiu-se, ainda, o objetivo específico analisar necessidades de regulamentação, em nível nacional, no tocante ao uso de sistemas de IA para triagem em telemedicina por planos de saúde privados e Sistema Único de Saúde – SUS. Embora, frise-se, não se espera que tais órgãos deliberem sobre as minúcias de sistemas informacionais, entende-se que implicações de usos de IA's em atendimentos em saúde devem estar em seus horizontes.

A pergunta que norteou este estudo foi: há bases legais, no Brasil, para implementação de sistemas de IA em teletriagem de pacientes? Verificou-se, nesse sentido, que o país já conta com marcos importantes, notadamente a LGPD, que cria bases sobre o tema no que tange à proteção de dados pessoais sensíveis, categoria na qual se incluem os dados pessoais de saúde. A legislação que regulamentou e autorizou a telessaúde no Brasil, a lei n.14.510, de 2022 traz alguns parâmetros e princípios que devem ser observados para a prática de telessaúde. A própria Constituição Federal de 1988 é um pilar importante no que se refere a assegurar, aos brasileiros, o direito ao acesso à saúde, amplo e gratuito. Face á necessidade crescente de ampliar tal direito à totalidade da população e, concomitante, otimizar custos no setor, ferramentas do tipo são potencialmente benéficas aos interesses coletivos.

No que se refere ao desenvolvimento e adoção de IA's, analisou-se o PL 21/2020, que versa sobre o assunto, ainda que não diretamente relacionado ao uso de IA no contexto de saúde. As diretrizes do documento, embora abrangentes, visam ao bem-estar social. Este deve se dar em estreita relação com o desenvolvimento econômico e o avanço tecnológico. Além disso enfatiza o respeito à dignidade humana, conceito que abarca atendimento em saúde, seja de maneira presencial, seja via recursos tecnológicos.

A telemedicina, convém reforçar, é um legado da pandemia que se consolida como uma realidade no país. Ocorre, no entanto, que o mercado de tecnologias voltadas à saúde, que não apenas defende, mas também comercializa soluções de IA para diagnóstico e triagem de pacientes atendidos no contexto da telemedicina, anda a passos mais largos que a legislação nacional. De maneira geral, ou seja, não restrito ao âmbito da saúde, a adoção de IA's está acelerada no contexto contemporâneo. Um caso claro que exemplifica o exposto é a ferramenta ChatGPT, da empresa OpenAI, que em pouquíssimas semanas após o seu lançamento, em novembro de 2022, tornou-se amplamente difundida e utilizada.

É evidente que tais tecnologias têm muito a oferecer à sociedade e, em particular, à saúde coletiva e não se pode refrear o avanço de atendimento à saúde, direito consagrado pela Constituição Federal de 1988 ao povo brasileiro. O que se observa, no entanto, neste recorte investigativo, é a vacância de regulamentação específica para o tema da teletriagem em saúde por IA no contexto normativo nacional. Assim, considera-se urgente atenção ao tema, uma vez que é atinente a uma demanda social por atendimento em saúde e que envolve não apenas o desenvolvimento tecnológico, mas também convoca setores de educação para o preparo técnico de profissionais e também de futuros usuários dessas tecnologias. Salienta-se, por fim, que o tema da teletriagem por robôs carece de atenção especial, nos documentos analisados, no que se refere à proteção de dados pessoais sensíveis em saúde.

REFERÊNCIAS

ACOSTA, Aline Marques; DURO, Carmen Lucia Mottin; LIMA, Maria Alice Dias da Silva. Atividades do enfermeiro nos sistemas de triagem/classificação de risco nos serviços de urgência: revisão integrativa. **Rev Gaúcha Enferm**, [S.l.], v. 33, n. 4, p. 181-190, dez. 2012. Disponível em: <https://doi.org/10.1590/S1983-14472012000400023>. Acesso em: 15 jan. 2023.

BERNASIUK, Helen Lentz Ribeiro. **Liberdade de pesquisa genética humana e a necessidade de proteção dos dados genéticos**. Rio de Janeiro: Lumen Juris, 2021. BRASIL, Ministério da Ciência, Tecnologia e Inovações. **Estratégia Brasileira de Inteligência Artificial – EBIA**. Disponível em: <https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/inteligencia-artificial>. Acesso em: 05 fev. 2023.

COMISSÃO EUROPEIA. Grupo Europeu de Ética na Ciência e Novas Tecnologias. **Declaração de Inteligência Artificial, Robótica e Sistemas 'Autônomos'**. Bruxelas, 9 de março de 2018. Disponível em: http://ec.europa.eu/research/ege/pdf/ege_ai_statement_2018.pdf. Acesso em: 8 fev. 2023.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [2016]. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 1 ago. 2022.

BRASIL. **Lei n. 13.989, de 15 de abril de 2020**. Dispõe sobre o uso da telemedicina durante a crise causada pelo coronavírus (SARS-CoV-2). Brasília: Presidência da República, 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/L13989.htm#derrubadaveto. Acesso em: 15 out. 2022.

BRASIL. Palácio do Planalto. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados (LGPD). Brasília: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 22 abr. 2022.

BRASIL. Palácio do Planalto. **Lei n. 14.510, de 27 de dezembro de 2022**. Altera a Lei nº 8.080, de 19 de setembro de 1990, para autorizar e disciplinar a prática da telessaúde em todo o território nacional, e a Lei nº 13.146, de 06 de julho de 2015; revoga a Lei nº 13.989, de 15 de abril de 2020. Brasília: Presidência da República, 2022. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/lei/L14510.htm#:~:text=LEI%20N%C2%BA%2014.510%2C%20DE%2027,15%20de%20abril%20de%202020. Acesso em: 16 mar. 2023.

BRASIL. **Projeto de Lei n. 21/2020**. Estabelece fundamentos, princípios e diretrizes para o desenvolvimento e a aplicação da inteligência artificial no Brasil; e dá outras providências. Brasília: Senado Federal, 2020. Disponível em: <https://www.camara.leg.br/propostas-legislativas/2236340>. Acesso em: 05 fev. 2023.

CABRINI, Natália. 6 Tendências da Telemedicina no Brasil em 2022. **Medicina S/A**, [s.l.], 03 mai. 2022. Disponível em: <https://medicinas.com.br/6-tendencias-telemedicina/>. Acesso em: 15 out. 2022.

CONSELHO FEDERAL DE ENFERMAGEM. **Resolução n. 696, de 2022**. Dispõe sobre a atuação da Enfermagem na Saúde Digital, normatizando a Telenfermagem. Brasília: COFEN, 2022. Disponível em: http://www.cofen.gov.br/resolucao-cofen-no-696-2022_99117.html. Acesso em: 15 out. 2022.

CONSELHO FEDERAL DE MEDICINA. **Resolução n. 2.314, de 2022**. Define e regulamenta a telemedicina, como forma de serviços médicos mediados por tecnologias de comunicação. Brasília: CFM, 2022. Disponível em: https://sistemas.cfm.org.br/normas/arquivos/resolucoes/BR/2022/2314_2022.pdf. Acesso em: 15 out. 2022.

FREITAS, Juarez. **Direito e inteligência artificial: em defesa do humano**/ Juarez Freitas, Thomas Bellini Freitas. Belo Horizonte: Fórum, 2020.

FINCATO, Denise Pires; GILLET, Sérgio Augusto da Costa. **A pesquisa jurídica sem mistérios**: do projeto de pesquisa à banca. 3. ed. rev. e atual. Porto Alegre: Editora Fi, 2018.

GIGLIO-JACQUEMOT, A. Etnografia da triagem. *In*: _____. Urgências e emergências em saúde: perspectivas de profissionais e usuários [online]. Rio de Janeiro: Editora FIOCRUZ, 2005. p. 45-55. Antropologia e Saúde collection. Disponível em: <https://doi.org/10.7476/9788575413784.0005>. Acesso em: 15 out. 2022.

LOBO, Luiz Carlos. Inteligência artificial, o Futuro da Medicina e a Educação Médica. **Revista Brasileira De Educação Médica**, [S.l.], v. 42, n. 3, p. 3-8, 2018. Disponível em: <https://doi.org/10.1590/1981-52712015v42n3RB20180115EDITORIAL1>. Acesso em: 15 jan. 2023.

LOBO, L. C. Inteligência Artificial e Medicina. **Revista Brasileira De Educação Médica**, [S.l.], v. 41, n. 2, p. 185-193, 2017. Disponível em: <https://doi.org/10.1590/1981-52712015v41n2esp>. Acesso em: 15 jan. 2023.

MORALES, Hugo M. P. *et al.* COVID-19 in Brazil—Preliminary Analysis of Response Supported by Artificial Intelligence in Municipalities. **Front. Digit. Health**, [s.l.], v. 3, n. 648585, p. 1-6, jun. 2021. Disponível em: <https://www.frontiersin.org/articles/10.3389/fdgth.2021.648585/full>. Acesso em: 15 out. 2022. doi: 10.3389/fdgth.2021.648585

NUNES, H. da C.; GUIMARÃES, R. M. C.; DADALTO, L. Desafios bioéticos do uso da inteligência artificial em hospitais. **Revista Bioética**, [S.l.], v. 30, n. 1, p. 82-93, 2022. Disponível em: <https://doi.org/10.1590/1983-80422022301509PT>. Acesso em: 15 jan. 2023.

ORGANIZAÇÃO PAN-AMERICANA DA SAÚDE. OMS publica primeiro relatório global sobre inteligência artificial na saúde e seis princípios orientadores para sua concepção e uso. Site OPAS, [s.l.], 28 jun. 2021. Disponível em: <https://www.paho.org/pt/noticias/28-6-2021-oms-publica-primeiro-relatorio-global-sobre-inteligencia-artificial-na-saude-e>. Acesso em: 15 out. 2022.

ROSA, Giovanni Santa. ChatGPT lança API para empresas que querem colocar IA em seus apps. **Tecnoblog**, [S.l.], 01 de março de 2023. Disponível em: <https://tecnoblog.net/noticias/2023/03/01/chatgpt-lanca-api-para-empresas-que-querem-colocar-ia-em-seus-apps/>. Acesso em: 02 mar. 2023.

RUARO, Regina Linden; REIS, Ludimila Camilo Catão Guimarães. Los retos del desarrollo ético de la Inteligencia Artificial. **Veritas**, v. 65, n. 3, 2020. Disponível em: <https://dialnet.unirioja.es/servlet/articulo?codigo=8086046>. Acesso em 17 ago. 2022.

SOSTER, C. B. *et al.* Protocolos de triagem avançada no serviço de emergência: revisão sistemática e metanálise. **Rev. Latino-Am. Enfermagem**, [S.l.], v. 30, p. 1-12, 2022. Disponível em: <https://www.scielo.br/j/rlae/a/H7Dr5Gn6TrvjmX8gk5LpCrw/?format=pdf&lang=pt>. Acesso em: 15 jan. 2023.

TEIXEIRA, João de Fernandes. **O que é inteligência artificial** (recurso eletrônico). Porto Alegre, RS: Editora Fi, 2017.

11. A GARANTIA DO DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS NEURAIIS NO BRASIL: DESAFIOS E PERSPECTIVAS

*THE GUARANTEE OF THE FUNDAMENTAL RIGHT TO NEURAL DATA
PROTECTION IN BRAZIL: CHALLENGES AND PERSPECTIVES*



<https://doi.org/10.36592/9786554600552-11>

*Silvana Sampaio Arguelho*¹

*Fernando Medici*²

Orientador: Professor Dr. *Giovani Agostini Saavedra*³

RESUMO

O objetivo deste artigo é fazer uma abordagem inicial sobre o tema relativo à proteção dos dados neurais, dada a sua relevância no contexto acadêmico tanto no Brasil quanto no exterior. Inúmeros são os desafios éticos e jurídicos relacionados à privacidade e à autonomia dos indivíduos a serem enfrentados na era digital, incluída aqui a possibilidade de implementação de mecanismos de controle e transparência no uso da neurotecnologia. O texto abordará o tema sob uma perspectiva jurídica e

¹ Mestre em Direito Processual Penal pela Faculdade de Direito da Universidade de São Paulo. Doutoranda em Direito Político e Econômico pela Universidade Presbiteriana Mackenzie. Pesquisadora do Grupo de Pesquisa Governança Corporativa, Compliance & Proteção de Dados, da Universidade Presbiteriana Mackenzie (dgp.cnpq.br/dgp/espelhogrupo/8626442026609894). Advogada. Membro efetivo da Comissão Permanente de Direitos Humanos e da Comissão Especial de Privacidade, Proteção de Dados e Inteligência Artificial da OAB/SP.

<https://lattes.cnpq.br/1982614985619878>. contatosilvanaarguelho@gmail.com

² Graduado em Direito (Universidade Presbiteriana Mackenzie). Pós-Graduado em Direito Penal Econômico (Fundação Getúlio Vargas). Mestre e Doutorando em Direito Político e Econômico pela Universidade Presbiteriana Mackenzie. Pesquisador do Grupo de Pesquisa Governança Corporativa, Compliance & Proteção de Dados da Universidade Presbiteriana Mackenzie (dgp.cnpq.br/dgp/espelhogrupo/8626442026609894). Advogado e escritor.

<http://lattes.cnpq.br/2843737543682264>. fernandomgm@gmail.com

³ Professor da *Universidade Presbiteriana Mackenzie* – SP (Doutorado, Mestrado, MBA e Graduação). Doutor em Direito e Filosofia pela *Johann Wolfgang Goethe - Universität Frankfurt am Main* (Alemanha). Mestre em Direito pela *Pontifícia Universidade Católica do Rio Grande do Sul* (PUCRS). Líder do Grupo de Pesquisa Governança Corporativa, Compliance & Proteção de Dados, registrado no CNPq e homologado pela Universidade Presbiteriana Mackenzie – SP. Membro da Comissão de *Compliance* do Conselho Federal da OAB. Presidente do Instituto Auditoria, Riscos e *Compliance* (ARC) e da Associação Brasileira de Auditoria, Riscos e *Compliance* (ABRARC). Sócio-Fundador e *Head de Compliance e Direito Digital da Saavedra & Gottschefsky* – Sociedade de Advogados.

por meio de uma análise comparativa do direito. Como se trata de um assunto ainda pouco explorado na literatura, este trabalho pretende investigar a atual situação regulatória da proteção da mente em nível internacional e as iniciativas em andamento no âmbito nacional. Essa reflexão se torna fundamental para estabelecer alguns fundamentos teóricos essenciais que permitam dar seguimento a um debate mais aprofundando sobre essa relevante temática.

Palavras-chave: Inteligência artificial. Neurodireito. Ética. Tecnologia. Legislação.

ABSTRACT

The purpose of this article is to make an initial approach to the topic of neural data protection, given its relevance in the academic context both in Brazil and abroad. There are many ethical and legal challenges related to privacy and the autonomy of individuals to be faced in the digital age, including the possibility of implementing control mechanisms and transparency in the use of neurotechnology. The text will approach the subject from a legal perspective and through a comparative analysis of the law. As this is a subject that has been little explored in the literature, this paper intends to investigate the current regulatory situation of mind protection at the international level and the initiatives underway at the national level. This reflection becomes fundamental to establish some essential theoretical foundations that allow the continuation of a deeper debate on this relevant m, ,kk, subject.

Keywords: Artificial Intelligence. Neurolaw. Ethics. Technology. Legislation.

INTRODUÇÃO

A proteção dos dados pessoais é uma questão cada vez mais relevante no Brasil e no mundo todo. No Brasil, a Lei Geral de Proteção de Dados Pessoais (LGPD), em vigor desde 18 de setembro de 2020, estabelece regras claras para a coleta, uso, armazenamento e compartilhamento de dados pessoais, considerados como sendo aqueles que possibilitam a identificação, direta ou indireta, da pessoa natural (artigo 5º, inciso I, da Lei nº 13.709/2018).

Dentre os dados pessoais, há aqueles que exigem maior atenção no tratamento: os relacionados a crianças e adolescentes (artigo 14 e seguintes da Lei

nº 13.709/2018); e os "sensíveis" (artigo 5º, inciso II, da Lei nº 13.709/2018), que são os que revelam origem racial ou étnica, convicções religiosas ou filosóficas, opiniões políticas, filiação sindical, questões genéticas, biométricas e sobre a saúde ou a vida sexual de uma pessoa.

A coleta e o armazenamento de informações pessoais por empresas e governos são progressivos e dinâmicos, ao ponto do acesso a tais dados ter chegado ao cérebro humano. São os chamados dados neurais ou dados mentais, expressos, justamente, nas informações geradas pelos sistemas neurais.

No contexto da tecnologia da informação, a análise dos dados neurais relaciona-se, por exemplo, com a aplicação de técnicas de aprendizado de máquina e inteligência artificial para entender e prever o comportamento humano com base em dados coletados por meio de dispositivos eletrônicos e sensores.

Com o avanço da inovação de inteligência artificial, em especial das redes neurais, o uso desse tipo de dado em diversas áreas, como saúde, finanças, publicidade e segurança, vem se tornando cada vez mais comum, situação que acaba por suscitar preocupações em relação à privacidade, segurança e transparência, dentre outros.

Com isso, a pergunta que não quer calar é no sentido de verificarmos a questão em torno da necessidade de regulamentação dos dados neurais, voltada para a garantia do tratamento lícito, ético e responsável dos mesmos, incentivando a transparência e a responsabilidade por parte dos desenvolvedores de sistemas de inteligência artificial, aumentando a confiança na tecnologia e seu potencial de benefício para a sociedade visando, acima de tudo, a proteção dos direitos dos indivíduos, evitando-se abusos por parte de empresas e governos.

À vista desse cenário, uma investigação sobre o grau de proteção dos dados neurais que o atual ordenamento jurídico nacional lhe confere (ainda que em termos de iniciativas preliminares), e se o mesmo pode ser considerado satisfatório ou não, isto é, se tem o condão de fornecer todos esses elementos que traduzem o correto processamento dos dados, protegendo a integridade física e a segurança psíquica do indivíduo em relação ao avanço das neurotecnologias, torna-se premente.

1. DADOS NEURAIIS. CONCEITO

Os dados neurais são uma realidade na era digital em que vivemos. Trata-se de informações processadas ou geradas por modelos de redes neurais artificiais que se baseiam na estrutura e funcionamento do cérebro humano.

Estamos diante de uma progressiva capacidade da tecnologia em medir não só parâmetros físicos, mas também informações relacionadas às faculdades mentais, como processos cognitivos, preferências pessoais e estados afetivos. Embora ainda não seja possível decodificar todo o conteúdo dos estados mentais, algumas desses aparatos digitais, como interfaces neurais, sistemas de computação afetiva e comportamental, permitem estabelecer associações estatísticas entre padrões de dados e comportamentos mentais. Além disso, a análise do big data possibilita explorar essas atividades em tempo real e de maneira preditiva. A ideia de "dados mentais" está relacionada, destarte, com qualquer tipo de dado que possa ser organizado e processado para inferir os estados mentais de uma pessoa, incluindo estados cognitivos, afetivos e conativos (IENCA; MALGIERI, 2022).

Esses modelos são aptos a aprender padrões e relações complexas em dados, permitindo sua aplicação em diversas áreas como reconhecimento de fala, imagens, linguagem natural e outras. Para treinar esses modelos, são utilizados dados neurais gerados a partir de diversas fontes, como imagens, textos, áudios, sensores, entre outros, que são alimentados às redes neurais de modo a aprenderem a realizar tarefas específicas.

O uso de dados neurais pode ter implicações em diversas áreas, como na área de marketing, por exemplo, onde a análise de dados neurais é capaz de subsidiar as empresas na avaliação de tendências e preferências dos consumidores, personalizando, assim, as campanhas publicitárias. Na área da saúde, o uso de dados neurais tem o potencial de ir desde a condução de pesquisas médicas até o diagnóstico e tratamento de diversas doenças, inclusive as mais complexas possíveis.

Outra aplicação importante dos dados neurais é a melhoria de sistemas de reconhecimento de voz e imagens, além da tradução automática de idiomas.

Entretanto, é importante destacar que o processamento de dados neurais envolve, na maioria das vezes, informações pessoais extremamente sensíveis, detendo um potencial valioso para processar um considerável volume de informações e encontrar padrões e relações intrincados dentro deles.

Ante esse panorama, é fundamental garantir que o tratamento dos dados neurais seja realizado de forma ética e legal, observando-se as normas e diretrizes em vigor para a proteção da privacidade e da segurança das informações envolvidas.

Nesse sentido, mister que as empresas, organizações e instituições que utilizam dados neurais estejam cientes das questões éticas e de privacidade envolvidas no seu uso e adotem medidas adequadas e efetivas para garantir a sua segurança e integridade, resguardando os direitos fundamentais e a liberdade dos respectivos titulares.

Porém, para que isso seja possível, é preciso avaliar se o nosso ordenamento jurídico atual propicia as ferramentas necessárias para lidar com a complexidade dessas questões. Isso significa que precisamos investigar se, na atualidade, contamos com leis e regulamentações adequadas que ofereçam proteção suficiente aos titulares de dados neurais.

2. BREVES CONSIDERAÇÕES SOBRE A QUESTÃO DA PROTEÇÃO DE DADOS NEURAIIS NO BRASIL

Encontra-se em análise perante a Câmara dos Deputados o Projeto de Lei nº 522/2022⁴ que propõe a regulamentação da proteção do uso e tratamento de dados neurais, obtidos diretamente ou indiretamente da atividade do sistema nervoso central, por meio de interfaces cérebro-computador ou outras tecnologias invasivas ou não-invasivas.

O texto propõe a inclusão dessas medidas no próprio bojo da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), conceituando o que é um dado neural e regulamentando a sua proteção para fins de assegurar o direito à privacidade mental, à identidade e autonomia pessoal, ao livre arbítrio e

⁴ BRASIL. Câmara dos Deputados. Projeto de Lei nº 522/2022. Disponível em: <https://www.camara.leg.br/propostas-legislativas/2317524>. Acesso em: 20 set. 2022.

autodeterminação, ao acesso equitativo ao aumento cognitivo, e o direito à proteção contra a discriminação algorítmica ou as decisões tomadas, prevendo, outrossim, que o tratamento de dados neurais somente ocorrerá com o consentimento específico e destacado do titular ou responsável legal para finalidades próprias.

O projeto também veda o uso de qualquer interface cérebro-computador que possa causar danos à identidade individual, autonomia ou integridade psicológica do titular dos dados.⁵

⁵ Segundo o projeto de lei apresentado, o art. 5º da Lei nº 13.709, de 14 de agosto de 2018, passaria a vigorar com as seguintes alterações:

“Art. 5º

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, dado neural, quando vinculado a uma pessoa natural;

.....
XX - dado neural: qualquer informação obtida, direta ou indiretamente, da atividade do sistema nervoso central e cujo acesso é realizado por meio de interfaces cérebro-computador, ou qualquer outra tecnologia, invasivas ou não-invasivas;

XXI - interface cérebro-computador: qualquer sistema eletrônico, óptico ou magnético que colete informação do sistema nervoso central e a transmita a um sistema informático ou que substitua, restaure, complemente ou melhore a atividade do sistema nervoso central em suas interações com o seu ambiente interno ou externo;

XXII - neurotecnologia: conjunto de dispositivos, métodos ou instrumentos não farmacológicos que permitem uma conexão direta ou indireta com o sistema nervoso.”

De outro lado, o Capítulo II da Lei nº 13.709, de 14 de agosto de 2018, passaria a vigorar acrescido da seguinte Seção II-A: “Seção II-A Do Tratamento de Dados Neurais.

Art. 13-A O tratamento de dados neurais somente ocorrerá quando:

I - o titular ou o responsável legal consentir, de forma específica e destacada, para finalidades específicas, mesmo em circunstâncias clínicas ou nos casos em que a interface cérebro-computador tenha a capacidade de tratar dados com o titular inconsciente;

II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

a) realização de estudos por órgão de pesquisa, garantida a anonimização dos dados pessoais sensíveis;

b) proteção da vida ou da incolumidade física do titular ou de terceiro;

c) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

Parágrafo único. O pedido de consentimento para o tratamento de dados neurais deve indicar, de forma clara e destacada, os possíveis efeitos físicos, cognitivos e emocionais de sua aplicação, as contraindicações bem como as normas sobre privacidade e as medidas de segurança da informação adotadas.

Art. 13-B É vedado o uso de qualquer interface cérebro-computador ou método que possa causar danos à identidade individual do titular dos dados, prejudicar sua autonomia ou sua integridade psicológica.

Art. 13-C É vedada a comunicação ou o uso compartilhado entre controladores de dados neurais com objetivo de obter vantagem econômica.

Art. 13-D Não se aplicam aos dados neurais as exceções previstas no inciso I e inciso II, alínea ‘a’, do art. 4º.

Art. 13-E O Estado tomará medidas para assegurar o acesso equitativo aos avanços da neurotecnologia”.

Na atualidade, o texto encontra-se submetido a exame perante as comissões de Seguridade Social e Família, de Ciência e Tecnologia, Comunicação e Informática, e de Constituição e Justiça e de Cidadania.

A justificativa do mencionado projeto de lei discute, em síntese, o potencial impacto da neurotecnologia⁶ no tratamento de dados pessoais, esclarecendo que embora ela possa trazer benefícios para a humanidade (como são os chamados implantes cocleares e o caso David Mzee⁷), a coleta de dados diretamente do cérebro humano pode subverter completamente a privacidade e a forma como interagimos com o ambiente externo.

Nesse sentido, o texto discorre que os dados neurais⁸ são uma propriedade que independe do meio e podem ser materializados pelo cérebro ou em material inorgânico, configurando uma característica semântica ou de linguagem com o cérebro. As informações neurais são consideradas dados pertencentes exclusivamente ao domínio do cérebro, e a coleta, compartilhamento e processamento de dados neurais são capazes de afetar não apenas a privacidade, mas também a integridade psicológica do titular.

A justificativa ressalta, por exemplo, o fato de que as diversas interfaces entre cérebros e computadores vêm sendo desenvolvidas, independentemente de cirurgia, pois conseguem ser "vestidas" como um acessório externo, o que pode levar a uma adoção massiva dessas tecnologias pela população, permitindo que Estados e empresas tratem dados extremamente sensíveis. Existe uma quantidade

⁶ A neurotecnologia aqui entendida como sendo um campo da ciência e engenharia que desenvolve métodos para conectar o sistema nervoso a computadores ou máquinas.

⁷ A justificativa se reporta aos implantes cocleares, popularmente conhecidos como ouvidos biônicos. Esses dispositivos são implantados dentro do ouvido e transformam sinais acústicos em ondas elétricas, estimulando o nervo auditivo e devolvendo a audição para aquelas pessoas que não conseguem se beneficiar de aparelhos auditivos comuns. Destaca, outrossim, que em 2018, também ficou famoso o caso de David Mzee, um tetraplégico que voltou a andar curtas distâncias, com o auxílio de um andador ortopédico, graças ao implante de eletrodos que reanimaram sua medula espinhal.

⁸ O projeto de lei esclarece que "os dados neurais não se confundem com dados biométricos pois não constituem órgãos ou tecidos corporais. Dados neurais são uma propriedade que independe do meio e podem ser materializados pelo cérebro ou em material inorgânico, configurando uma característica semântica, ou de linguagem, com o cérebro. Nesse sentido, essas informações constituem dados pertencentes unicamente ao domínio do cérebro. Os mecanismos de operação dos neurônios transmitem sinais recheados de informações sobre o estado neurocognitivo da pessoa. Por isso, pelo fato de os dados neurais constituírem parte da mente das pessoas, o titular deve ter direito de proteção não apenas a sua privacidade, mas também a sua integridade psicológica".

significativa de técnicas de neuroimagem, como a tomografia computadorizada, que medem e deduzem a atividade cerebral.

O texto alerta para circunstâncias significativas, tais como:

- A tecnologia está transformando a realidade de maneira acelerada e em breve, os algoritmos serão capazes de programar as pessoas. Isso levanta questões éticas e jurídicas importantes que precisam ser abordadas para garantir que os avanços tecnológicos sejam benéficos para a sociedade como um todo;

- As empresas poderão criar algoritmos que não apenas extraiam dados do cérebro, mas também aumentem a capacidade cognitiva das pessoas. Essa possibilidade de melhorar a capacidade cognitiva pode levar à criação de castas, o que pode agravar as desigualdades sociais;

- É preciso garantir que a população se beneficie do progresso científico, e não que as desigualdades sociais se agravem ainda mais. Para isso, torna-se imprescindível a implementação de medidas regulatórias que permitam que os avanços tecnológicos sejam utilizados para melhorar a vida das pessoas, sem criar novos problemas sociais;

- Deve-se proibir intervenções no cérebro que possam determinar os sentimentos, desejos, pensamentos e paixões das pessoas, de forma a garantir que as sociedades democráticas continuem funcionando de maneira saudável, evitando-se que a tecnologia seja utilizada para controlar as pessoas de forma indevida.

Com isso, foi enfatizada a necessidade de se desenvolver uma nova estrutura regulatória que, no mínimo, venha a assegurar: a) o direito à privacidade mental; b) o direito à identidade e autonomia pessoal; c) o direito ao livre arbítrio e autodeterminação; d) o direito ao acesso equitativo ao aumento cognitivo; e e) o direito à proteção contra a discriminação algorítmica ou as decisões tomadas.

O projeto de lei destaca que a proteção da integridade, da privacidade e da identidade mental em relação ao desenvolvimento das neurotecnologias dá origem, assim, aos chamados neurodireitos, situação essa que resulta na exigência de se atribuir aos dados neurais uma proteção superior à atualmente destinada aos dados sensíveis.

Em resumo, a justificativa anuncia a imprescindibilidade de proteção dos dados neurais, à vista dos riscos que o uso indevido deles pode representar para a

privacidade e a integridade psicológica dos indivíduos. O projeto de lei busca estabelecer uma regulamentação adequada para a coleta, processamento e compartilhamento de dados neurais, a fim de garantir a sua proteção como um direito fundamental autônomo.

Importa pontuar, outrossim, que a proposta em apreço foi inspirada no projeto de lei chileno. Porém, enquanto no Chile houve, na época, a propositura de um projeto de lei autônomo para tratar do tema, a nível constitucional, no caso brasileiro, a ideia inicial é no sentido de regulamentar os neurodireitos no bojo da Lei Geral de Proteção de Dados, ao argumento de que a despeito da necessidade de maior proteção aos dados neurais, há uma credulidade no sentido de que os princípios da LGPD serão úteis para tal finalidade.⁹

Ou seja, diversamente da legislação chilena, o projeto de lei brasileiro optou, em um primeiro momento, por tratar da proteção dos dados neurais na própria LGPD, e não através de uma lei específica, tampouco uma emenda constitucional.

3. A PROTEÇÃO DOS DADOS NEURAIIS NO ÂMBITO INTERNACIONAL

3.1. A INICIATIVA CHILENA

A Lei Chilena promoveu uma reforma constitucional inédita (nº 21.383, de 25 de outubro de 2021) alterando o disposto no artigo 19, número 1, da Constituição Política da República¹⁰, “para colocar o desenvolvimento científico e tecnológico a serviço do povo”, passando a proteger a atividade cerebral e a informação, tornando-

⁹ O trecho apresentado na justificativa foi o seguinte: “Dentre os vários países que começaram a debater os chamados neurodireitos, é o Chile que parece estar mais adiantado, havendo sido apresentado um projeto de lei e uma proposta de emenda à constituição naquele país com o fim de regulamentá-los. A presente proposta é inspirada no projeto de lei chileno, com uma diferença importante. Lá, foi proposto um projeto de lei autônomo para tratar do tema. Aqui, a ideia inicial é cuidar dos neurodireitos na Lei Geral de Proteção de Dados. Embora acredite que os dados neurais precisem ainda de maior proteção, penso que os princípios da LGPD serão úteis para tratar da matéria”.

¹⁰ Eis o teor do mencionado artigo 19, n 1, da Carta Fundamental Chilena: “O desenvolvimento científico e tecnológico estará a serviço das pessoas e será realizado com respeito à vida e à integridade física e mental. A lei regulará os requisitos, condições e restrições para seu uso em pessoas e deve proteger especialmente a atividade cerebral, bem como as informações dela”.

se, assim, o primeiro país do mundo a legislar sobre neurotecnologia que pode manipular a mente.

A primeira etapa da tramitação da reforma constitucional foi realizada perante o Senado, por meio de sua Comissão de Desafios Futuros. No trâmite constitucional na Câmara dos Deputados, com base no relatório elaborado pela Comissão de Futuro, Ciência, Tecnologia, Conhecimento e Inovação, a discussão centrou-se na precisão dos termos utilizados na redação da reforma, resultando em mudanças importantes na redação. O alcance da disposição foi estendido a qualquer tipo de desenvolvimento científico e tecnológico, com o objetivo de ampliar a proteção não apenas no que diz respeito ao uso de neurotecnologias. Eliminou-se, outrossim, qualquer referência que pudesse ser entendida como um novo direito fundamental e os únicos direitos fundamentais aos quais o dispositivo se referiu foram a vida, a integridade física e mental (PAREDES; QUIROZ, 2022).

A tramitação da reforma constitucional visou proteger constitucionalmente a "integridade e indenização mental em relação ao avanço das neurotecnologias", vislumbrando-se a necessidade de abordar esse assunto diretamente no catálogo de direitos fundamentais diante do avanço das chamadas neurotecnologias e os riscos e impactos que isso pode acarretar para os direitos humanos, concluindo pela consagração de um novo direito à neuroproteção, ancorado na dignidade humana. Buscou-se que essa nova garantia constitucional apresentasse uma "textura aberta", correspondendo ao legislador seu desenvolvimento e delimitação, sem prejuízo de ter a proteção conferida pela ação constitucional (MIRALLES; BENOIT; KRAMCSÁK, 2021).

O direito à neuroproteção buscou proteção contra o avanço das neurotecnologias. Uma nova dimensão da dignidade humana, vinculada ao "cérebro humano", tanto em sua extensão física quanto em seu potencial mental, sendo que o conteúdo essencial desse direito foi identificado com "quatro prioridades éticas para neurotecnologias e inteligência artificial - IA : Primeiro, o direito à privacidade das informações produzidas pela atividade cerebral, que podem ser acessadas por meio da neurotecnologia (chamada privacidade e consentimento) ou proteção de neurodados; segundo, o direito à identidade pessoal e autodeterminação (referido como agência), tendo em vista que a neurotecnologia abre a possibilidade de anular

ou alterar a identidade das pessoas; terceiro, o direito à igualdade diante do aumento do poder cerebral (chamado aumento ou aperfeiçoamento mental), o que implicaria a necessidade de regular para evitar a iniquidade; e quarto, o direito de controle parcial dos algoritmos (chamado tendência) derivado de decisões tomadas por máquinas por meio de algoritmos de IA (MIRALLES; BENOIT; KRAMCSÁK, 2021).

De qualquer modo, oportuno elucidar que parte da doutrina estrangeira entende que a reforma constitucional chilena não constituiu uma inovação tão significativa, considerando, por exemplo, a necessidade de especificar o significado da cláusula que estabelece que: "[o] desenvolvimento científico e tecnológico estará a serviço do povo", bem como fornecer um conteúdo técnico à frase que protege a "atividade cerebral, bem como as informações provenientes dele", que parece ser a frase que poderia ser a parte mais inovadora da reforma. Porém, essa reforma constitucional estaria longe de consagrar qualquer novo direito fundamental de natureza autônoma; muito menos poderia ser atribuído o efeito de representar a consagração normativa da categoria teórica de neurodireitos (PAREDES; QUIROZ, 2022).

Outra ala da literatura, por sua vez, não vislumbrou com clareza a existência de uma verdadeira "razão de direito" que justificasse essa reforma constitucional, pontuando, para tanto, algumas críticas relacionadas à suposta relevância ou conveniência em se consagrar constitucionalmente o novo direito à neuroproteção, seja pela possibilidade de problemas de coerência regulatória com órgãos reguladores mais arraigados em determinado sistema, bem como pelo fato de ocasionar um cenário de "inflação de direitos" que acabaria por erodir direitos já reconhecidos, de modo que, essa vertente, ao contrário, alega que uma interpretação progressiva dos direitos já existentes, tecnologicamente neutra, deveria ser suficiente para alcançar uma expansão que protegesse adequadamente a autonomia e a integridade dos sujeitos no contexto do uso das novas tecnologias (MIRALLES; BENOIT; KRAMCSÁK, 2021).

De outro lado, relativamente ao debate sobre a regulação das neurotecnologias, tem-se um grupo que reivindica a presença essencial do direito constitucional, mediante uma nova leitura dos valores e princípios constitucionais para regulamentar a sociedade digital e garantir que a tecnologia beneficie a

humanidade e o meio ambiente. Ou seja, na sociedade digital seria de rigor reconfigurar o pacto constitucional para abordar o uso das novas tecnologias, bem como repensar os valores sociais que devem reger as infraestruturas tecnológicas, já que a tecnologia é coletivista e não entende o indivíduo. Destaca-se a relevância na proteção dos direitos fundamentais dos indivíduos diante do uso da tecnologia, estabelecendo limites legais, criando órgãos autônomos de vigilância ou controle e promovendo novos desenvolvimentos tecnológicos que protejam esses direitos (TELLO, 2021).

3.2. A RECOMENDAÇÃO SOBRE INOVAÇÃO RESPONSÁVEL EM NEUROTECNOLOGIA - ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO (OCDE)

A neurotecnologia é uma área de pesquisa e desenvolvimento que tem crescido significativamente nas últimas décadas, e que envolve a utilização de tecnologias avançadas para explorar o funcionamento do sistema nervoso, compreender doenças neurológicas e desenvolver novas terapias para tratar essas doenças.

A proteção dos dados neurais é um dos principais desafios éticos e de segurança relacionados à neurotecnologia, diante do seu potencial de coletar e armazenar grandes quantidades de dados sobre o cérebro humano, incluindo informações extremamente sensíveis, como pensamentos, emoções e comportamentos. Esses dados neurais podem ser usados para desenvolver novas terapias e tratamentos para doenças neurológicas, mas também podem ser usados indevidamente para manipulação e violação da privacidade.

Diante dessa perspectiva, a Organização para a Cooperação e Desenvolvimento Econômico (OCDE) aprovou em 11 de dezembro de 2019 uma Recomendação sobre Inovação Responsável em Neurotecnologia¹¹, que tem como objetivo orientar governos, pesquisadores, empresas e a sociedade em geral a abordar questões éticas, sociais e de segurança relacionadas à neurotecnologia e

¹¹ Disponível em: <https://www.oecd.org/science/recommendation-on-responsible-innovation-in-neurotechnology.htm>. Acesso em: 10 out. 2022.

que constituiu o primeiro padrão internacional neste domínio, promovendo a inovação no campo.¹²

De acordo com essa Recomendação o conceito de neurotecnologia está relacionado com “dispositivos e procedimentos utilizados para acessar, controlar, investigar, avaliar, manipular ou emular a estrutura e função dos sistemas neurais de pessoas físicas” (OCDE, 2019).

A Recomendação da OCDE aborda vários temas relevantes para a neurotecnologia, como privacidade e proteção de dados, segurança cibernética, uso de animais em pesquisas, uso de inteligência artificial em neurotecnologia, entre outros, e destaca a importância da privacidade e proteção de dados em relação à neurotecnologia (OCDE, 2019).

Ela afirma que é importante garantir que as informações pessoais dos usuários de neurotecnologias sejam protegidas e que os usuários tenham controle sobre como suas informações são coletadas, armazenadas e compartilhadas. Isso inclui o consentimento informado dos usuários para a coleta e uso de seus dados neurais (OCDE, 2019).

A Recomendação também aborda a segurança cibernética em relação à neurotecnologia, uma vez que a neurotecnologia é frequentemente usada em sistemas conectados à internet. Isso significa que há um risco de violação de segurança e acesso indevido aos dados neurais (OCDE, 2019).

Relativamente ao tópico que trata da proteção dos dados pessoais do cérebro e outras informações obtidas por meio da neurotecnologia, a Recomendação preconiza os seguintes deveres aos Membros e não Membros que tenham aderido ao documento Recomendação (intitulados “Aderentes”):

a) O fornecimento de informações claras ao público e aos participantes da pesquisa sobre a coleta, armazenamento, processamento e uso potencial de dados cerebrais pessoais coletados para fins de saúde (OCDE, 2019);

¹² A Recomendação incorpora em seu bojo nove princípios, que se concentram em: promover a inovação responsável, priorizar a avaliação de segurança, promover a inclusão, promover a colaboração científica, permitir a deliberação social, habilitar a capacidade de supervisão e órgãos consultivos, proteger dados cerebrais pessoais e outras informações, promover culturas de administração e confiança em todo o setor público e privado e antecipar e monitorar o uso não intencional e/ou uso indevido potencial.

b) Assegurar que existam meios de obtenção de consentimento adequados para proteger a autonomia dos indivíduos, incluindo a consideração de casos especiais de capacidade limitada de tomada de decisão (OCDE, 2019);

c) Promover oportunidades para que os indivíduos escolham como seus dados são usados e compartilhados, incluindo opções para acessar, alterar e excluir dados pessoais (OCDE, 2019);

d) Promover políticas que protejam os dados pessoais do cérebro de serem usados para discriminar ou excluir inadequadamente certas pessoas ou populações, especialmente para fins comerciais ou no contexto de processos legais, empregos ou seguros (OCDE, 2019);

e) Proteger as informações obtidas por meio da aplicação de neurotecnologia contra uso não autorizado, inclusive por meio do uso de acordos de acesso a dados, quando apropriado (OCDE, 2019);

f) Promover a confidencialidade e privacidade e mitigar brechas de segurança, inclusive por meio da implementação de rigorosos padrões de segurança (OCDE, 2019);

g) Assegurar não só a rastreabilidade dos dados recolhidos e tratados, mas também dos atos médicos em que a neurotecnologia é utilizada (OCDE, 2019).

3.3. A NEURORIGHTS FOUNDATION

A *NeuroRights Foundation*¹³, da Universidade de Columbia, atua na proteção dos direitos humanos de todas as pessoas contra o potencial uso indevido ou abuso da neurotecnologia, e estão trabalhando para incorporar cinco neurodireitos específicos que foram identificados como especialmente críticos na lei internacional de direitos humanos, estruturas legais e regulatórias nacionais e diretrizes éticas. São eles:

a) Privacidade mental: qualquer neurodado obtido da medição da atividade neural deve ser mantido privado. Se armazenado, deve haver o direito de excluí-lo a

¹³ Disponível em: <https://neurorightsfoundation.org/>. Acesso em 10 out. 2022.

pedido do sujeito. A venda, transferência comercial e uso de dados neurais devem ser estritamente regulamentados;

b) Identidade pessoal: Limites devem ser desenvolvidos para proibir que a tecnologia perturbe o senso de identidade. Quando a neurotecnologia conecta indivíduos com redes digitais, ela pode obscurecer a linha entre a consciência de uma pessoa e as entradas tecnológicas externas;

c) Livre arbítrio: Os indivíduos devem ter o controle final sobre sua própria tomada de decisão, sem manipulação desconhecida de neurotecnologias externas;

d) Acesso justo ao aprimoramento mental: Deve haver diretrizes estabelecidas em nível internacional e nacional que regulem o uso de neurotecnologias de aprimoramento mental. Estas orientações devem basear-se no princípio da justiça e garantir a igualdade de acesso;

e) Proteção contra preconceito: Contramedidas para combater o viés devem ser a norma para algoritmos em neurotecnologia. O design do algoritmo deve incluir entrada de grupos de usuários para abordar o viés fundamentalmente;

Além desse objetivo, a *NeuroRights Foundation* tem por escopo prevenir e reduzir o risco de uso indevido ou abuso da neurotecnologia. Como forma de coibir essa situação, eles estão elaborando uma estrutura ética para empreendedores, cientistas, empresas e investidores e outros que desenvolvem neurotecnologia chamada "Juramento TecnoCrata", cujo texto encontra-se em fase de elaboração. Do mesmo modo que os médicos devem seguir o juramento de Hipócrates, aqueles que desenvolvem e administram a neurotecnologia seriam instados a apoiar o "juramento tecnocrático".

4. OS DADOS NEURAI E O DILEMA BRASILEIRO

Vimos, até o presente momento, que o PL nº 522/2022 em trâmite no Congresso Nacional tem por objetivo tratar dos dados neurais no próprio bojo da LGPD, ao contrário do modelo Chileno, que optou por uma reforma constitucional. Por outro lado, abordamos a temática através de outras normas internacionais e que estão a servir de paradigma para o tema aqui examinado.

A questão que resta a ser enfrentada é se, ao invés de uma modificação no corpo da Lei nº 13.709/2018, nos moldes propostos pelo PL nº 522/2022, mister a elaboração de um projeto autônomo, em forma de Emenda Constitucional, que acrescentasse o direito à proteção de dados neurais no rol de direitos e garantias fundamentais do cidadão, tal como foi levado a efeito pela Constituição do Chile, de modo a permitir uma adequada governança desses dados.

O avanço das neurotecnologias é uma realidade que vem se multiplicando, nomeadamente com a aplicação de técnicas de inteligência artificial, considerando que os seus respectivos sistemas são responsáveis pela criação de muitas previsões, recomendações e decisões com as quais o ser humano acaba por interagir, muitas vezes, de forma direta.

E são justamente essas aplicações neurotecnológicas em seres humanos que levaram ao surgimento de um discurso cuja principal característica é a demanda por novos direitos que vêm sendo chamados de neurodireitos (ASÍS, 2022).

Daí, inclusive, a preocupação da literatura estrangeira em defender a necessidade de se proteger constitucionalmente a atividade e a informação cerebral contra o avanço dessas neurotecnologias (MIRALLES; BENOIT; KRAMCSÁK, 2021).

Essa preocupação não é de hoje, pois no ano de 2017 um grupo de cientistas¹⁴ publicou um artigo intitulado *Four ethical priorities for neurotechnologies and AI*, na revista científica *Nature*, defendendo "quatro prioridades éticas para neurotecnologias e IA"¹⁵ (YUSTE et al., 2017: 162-163)

De outro lado, parte da literatura estrangeira parte da premissa de que os neurodados são uma forma única de dados e que isso levantará questões para a aplicação da lei de proteção de dados. As questões podem surgir em dois níveis. No nível técnico legal, é incerto se as definições e mecanismos usados na estrutura de proteção de dados podem ser facilmente aplicados aos neurodados. Em um nível mais fundamental, pode haver interesses em neurodados, particularmente aqueles relacionados à proteção da mente; a estrutura não foi projetada para representar e

¹⁴ Podemos destacar o neurocientista Rafael Yuste e a especialista em ética Sara Goering como sendo os grandes expoentes do trabalho realizado.

¹⁵ São elas: **direito à privacidade mental, direito à identidade e autonomia pessoal, direito ao aumento cognitivo e direito de proteção contra vieses.**

pode ser insuficientemente equipada ou construída para lidar com eles (HALLINAN et al., 2014).

Contudo, em contraponto, há autores que veem com olhos céticos a conveniência em criar uma categoria de direitos humanos, ao argumento de que a maioria dos sistemas jurídicos nacionais e internacionais já protegem a liberdade, o consentimento, a igualdade, a integridade, a privacidade e a informação, bem como que a criação de novos direitos implicaria uma descrição geral e pouco exaustiva que sequer, efetivamente, regularia o avanço neurotecnológico. Como proposta alternativa, defendem preparar os operadores de justiça para interpretar adequadamente os direitos constitucionais, considerando os desafios apresentados pelas neurotecnologias (BORBÓN & BORBÓN, 2021).

Todavia, tal posicionamento é minoritário. Dada as profundas e rápidas transformações tecnológicas, laborais e sociais advindas de novas tecnologias neurais, inúmeros autores encontrados na pesquisa bibliográfica realizada apontam para a necessidade de proteção específica (HALLINAN et al., 2014; YUSTE et al., 2017; ASÍS, 2022).

Ainda que existam princípios e normas gerais de fato já tragam liberdade, o consentimento, a igualdade, a integridade, a privacidade e a informação; sua aplicação específica aos neurodireitos estaria sujeita ao campo da interpretação de determinados operadores do direito e agentes políticos, o que traria incertezas e insegurança jurídica sobre a matéria.

Sendo assim, mostra-se necessário gerar proteções específicas ao neurodireitos nos ordenamentos jurídicos. No caso particular do Brasil, os dispositivos atualmente vigentes na LGPD não abarcam a matéria de forma a proteger especificamente os neurodireitos, tomando por base aqueles listados pela *NeuroRights Foundation*, da Universidade de Columbia.¹⁶ Também parecem insuficientes para englobar todas as recomendações da OCDE.¹⁷

Nessa perspectiva, de acordo com parte da doutrina pátria, verifica-se que existe uma corrente de pensamento que defende a viabilidade de alteração do disposto no artigo 5º da Constituição Federal, a fim de incluir uma proteção

¹⁶ Ver item 3.3 deste artigo.

¹⁷ Ver item 3.2 deste artigo.

específica à mente humana no contexto das neurotecnologias. Essa medida visa garantir a integridade mental e a transparência algorítmica, acompanhando a evolução científica e tecnológica global e reafirmando o compromisso com o desenvolvimento responsável. Ao adotar essa postura, o Brasil se juntaria a outros países e demonstraria liderança na proteção da pessoa humana, seguindo recomendações de organismos internacionais como a OCDE (PINTARELLI, 2022).

Uma outra opinião é que a Constituição do Brasil pode ser usada para proteger os dados neurais, considerando o direito à vida previsto no *caput* do artigo 5º. Porém, é necessário que a proteção seja forte, com uma lei que cubra todos os aspectos da neurotecnologia e estabeleça explicitamente os neurodireitos, incluindo a padronização dos termos de consentimento, a criptografia obrigatória, restrição de acesso aos dados neurais compartilhados e combate às tendências perigosas. Nesse aspecto, portanto, o atual projeto de lei proposto para alterar a LGPD e incluir em seu bojo a questão da proteção jurídica dos dados neurais não seria suficiente para tratar adequadamente desse assunto (SAAVEDRA; FALQUEIRO, 2021).

De qualquer modo, não há como negar que existe um certo consenso em torno da questão da necessidade de proteção jurídica dos dados neurais, nomeadamente em razão do uso de algoritmos em investigações neurocientíficas, sendo que a LGPD não abrange todos os aspectos desses dados tão específicos. A entrada do 5G e a IoT aceleram o emprego dos dispositivos neurais, permitindo que indivíduos e organizações possam rastrear, induzir ou manipular a experiência mental de outras pessoas. É essencial compreender os limites éticos, técnicos e jurídicos dos neuroalgoritmos e mapear os possíveis danos à personalidade e ao livre desenvolvimento individual. Além dos danos pessoais, os custos sociais, políticos e sanitários ainda são desconhecidos e afetam a integridade dos indivíduos e do Estado de Direito (SARLET, 2022).

CONCLUSÕES

O grande desenvolvimento da neurotecnologia é uma realidade que, longe de ser atual, vem se anunciando ao longo dos anos e crescendo de forma ininterrupta

dentro de uma sociedade considerada informacional com diversas atividades, cuja maior fonte é, justamente, o processamento de dados, incluídos aqui os neurais.

A despeito dos benefícios trazidos com os avanços tecnológicos, principalmente, para a área da saúde, ainda não temos definidos os contornos legais em que o tratamento dos dados se opera, situação essa que pode ocasionar uma violação aos inúmeros direitos humanos e fundamentais.¹⁸

A discussão sobre a necessidade de proteção específica dos dados neurais é uma questão premente e que requer a atenção dos legisladores e da sociedade em geral. A modificação no corpo da Lei nº 13.709/2018, nos moldes propostos pelo PL nº 522/2022, pode não ser suficiente para assegurar a privacidade e os direitos fundamentais relacionados aos dados neurais. A elaboração de um projeto autônomo, em forma de Emenda Constitucional, que acrescente o direito à proteção de dados neurais no rol de direitos e garantias fundamentais do cidadão é uma alternativa a ser mais bem examinada, de modo a avaliar a viabilidade quanto à garantia adequada da governança desses dados.

De qualquer maneira, é fundamental que sejam estabelecidas normas claras para proteger os indivíduos e certificar que os avanços da neurotecnologia sejam feitos de forma ética e responsável. O Brasil, assim como outros países, deve estar atento às questões relacionadas aos neurodireitos para que seja capaz de lidar com as complexidades e desafios que essas novas tecnologias apresentam.

REFERÊNCIAS BIBLIOGRÁFICAS

ASÍS, Rafael de. Sobre la propuesta de los neuroderechos. **DERECHOS Y LIBERTADES: Revista de Filosofía del Derecho y derechos humanos**, n. 47, p. 51-70, 2022. Disponível em: <https://e-revistas.uc3m.es/index.php/DYL/article/view/6873/5469>. Acesso em: set. 2022.

BORBÓN, Diego; BORBÓN, Luisa. "A Critical Perspective on NeuroRights: Comments Regarding Ethics and Law." **Frontiers in human neuroscience**, vol. 15 703121. 25 Oct. 2021. Disponível em :

¹⁸ Dentre os quais podemos destacar: liberdade (cognitiva), dignidade humana, livre desenvolvimento da personalidade e a própria proteção de dados pessoais.

<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8573066/>. Acesso em: 02 out. 2022.

CHILE. **Constitución Política de La República**. 2005. Disponível em: https://www.camara.cl/camara/doc/leyes_normas/constitucion.pdf. Acesso em: 24 mar. 2023.

HALLINAN, Dara; SCHÜTZ, Philip; FRIEDEWALD, Michael; DE HERT, Paul. **Neurodata and Neuroprivacy: Data Protection Outdated?. Surveillance and Society**. 2014. Disponível em: <https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/neurodata>. Acesso em: 28 out. 2022.

HOFFMANN-RIEM, Wolfgang. A Proteção Jurídica Fundamental da Confidencialidade e da Integridade dos Sistemas Técnicos de Informação de Uso Próprio. **Direito Público, 2022**. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/6212>. Acesso em: set. 2022.

IENCA, Marcello; MALGIERI, Gianclaudio. Mental Data Protection and the GDPR. **Journal of Law and the Biosciences**, 2022. Disponível em: <https://ssrn.com/abstract=3840403> or <http://dx.doi.org/10.2139/ssrn.3840403>. Acesso em: set. 2022.

IENCA, Marcelo; ROBERTO, Andorno. Towards new human rights in the age of neuroscience and neurotechnology. **Life Sci Soc Policy 13**, 2017. Disponível em: <https://doi.org/10.1186/s40504-017-0050-1>. Acesso em: 20 out. 2022.

MACKENZIE, Catriona; WALKER, Mary. Neurotechnologies, personal identity and the ethics of authenticity. **In Springer Handbook of Neuroethics. Dordrecht: Springer**. pp. 373-92, 2015. Disponível em: <https://utpjournals.press/doi/10.3138/ijfab.13.1.06>. Acesso em: 03 out. 2022.

MARDEN, Carlos; MARTINS, Gabriela (Org.). **Direito e Neurociência - Além das Primeiras Impressões**. Juruá Editora: Curitiba. 2020.

MIRALLES, Danielle Zaror; BENOIT, Michelle Bordachar; KRAMCSÁK, Pablo Trigo. *Acerca de la necesidad de proteger constitucionalmente la actividad e información cerebral frente al avance de las neurotecnologías: Análisis crítico de la reforma constitucional introducida por la Ley 21.383*. **Revista Chilena De Derecho Y Tecnología, 10 (2)**, 1–10, 2021. Disponível em: <https://doi.org/10.5354/0719-2584.2021.65650>. Acesso em: ago. 2022.

NEURORIGHTS Foundation. Disponível em: <https://neurorightsfoundation.org/>. Acesso em: ago. 2022.

OECD. **Recommendation on Responsible Innovation in Neurotechnology**, 2019. Disponível em: <https://www.oecd.org/science/recommendation-on-responsible-innovation-in-neurotechnology.htm>. Acesso em: ago. 2022.

PAREDES, Felipe; QUIROZ, CATALINA. Neuroderechos en Chile: Estado del arte y desafíos. In **Neurodireito, neurotecnologia e direitos humanos**. Ana Maria D'Ávila Lopes [et al.] (organizadores); Aline Passos Maia [et al.]. Livraria do Advogado: Porto Alegre, 2022, p. 69-80.

PINTARELLI, Camila. A proteção jurídica da mente. **Revista de Direito da Saúde Comparado**, v. 1, n.1, p. 104-119, 2022.

RECHE TELLO, N. Nuevos derechos frente a la neurotecnología: la experiencia Chilena. **Revista de Derecho Político**, [S. l.], n. 112, p. 415–446, 2021. Disponível em: <https://revistas.uned.es/index.php/derechopolitico/article/view/32235>. Acesso em: 24 out. 2022.

SAAVEDRA, Giovani Agostini. Compliance de Dados. In: Doneda, Danilo; Sarlet, Ingo Wolfgang (et. all.). (Org.). **Tratado de Proteção de Dados Pessoais**. 1 ed. Rio de Janeiro: Forense, 2020, v. 1, p. 56-87.

SAAVEDRA, Giovani Agostini; FALQUEIRO, Bruno Laganá. Proteção Jurídica de Dados Neurais: Neural Data Legal Protection. In: Saavedra, Giovani (Org.). **Governança corporativa, compliance e proteção de dados**, 1 ed. São Paulo: Eseni Editora, vol. 2, 2021, p. 113/131.

SARLET, Gabrielle Bezerra Sales. **A proteção dos dados neurais sob o enfoque das neurociências e dos direitos humanos e fundamentais no contexto brasileiro**, 2022. Acessível em: <https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/362368/protecao-dos-dados-neurais-sob-o-enfoque-das-neurociencias>. Acesso em set. 2022.

SARLET, Ingo Wolfgang; SAAVEDRA, Giovani Agostini. **Fundamentos Jusfilosóficos e Âmbito de Proteção do Direito Fundamental à Proteção de Dados Pessoais**. Direito Público, Brasília, v. 17, n. pp. 33-57, 2020. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/4315/Sarlet%3B%20Saavedra%2C%202020>. Acesso em: 10 mar. 2022.

TELLO, Nuria Reche. *Nuevos derechos frente a la neurotecnología: la experiencia chilena*. **Revista De Derecho Político**, (112), 415–446, 2021. Disponível em: <https://doi.org/10.5944/rdp.112.2021.32235>. Acesso em set. 2022.

YUSTE, Rafael; GOERING, Sara; ARCAS, Blaise Agüera. et al. **Four ethical priorities for neurotechnologies and AI**. Nature 551, p. 159–163, 2017. Disponível em: <https://doi.org/10.1038/551159a>. Acesso em: 20 set. 2022.

12. SAÚDE PLANETÁRIA, EXTRAFISCALIDADE E O MANEJO DOS RESÍDUOS SÓLIDOS URBANOS¹

*PLANETARY HEALTH, EXTRAFISCALITY AND THE MANAGEMENT OF URBAN SOLID
WASTE*



<https://doi.org/10.36592/9786554600552-12>

Victória Maltchik Salles Jung²

RESUMO

O presente trabalho visa verificar como a extrafiscalidade pode auxiliar no correto manejo dos resíduos sólidos, atenuando a proliferação de doenças. A relevância do tema surge a partir do entendimento de que o direito à saúde, mesmo disposto no capítulo dos direitos sociais da Constituição Federal de 1988, pode ser lido enquanto um direito fundamental, mediante interpretação extensiva do direito à vida. A hipótese lançada é que a extrafiscalidade aparece como um forte estímulo às práticas sustentáveis na gestão do lixo, efetivando a promoção do direito fundamental à saúde, mais especificamente, investigar-se-á o âmbito coletivo.

Palavras-chave: Saúde planetária; Direitos Fundamentais; Extrafiscalidade; Resíduos Sólidos.

ABSTRACT

This paper aims to verify how the extrafiscal taxation can assist in the correct management of solid waste, mitigating the proliferation of diseases. The relevance of the theme arises from the understanding that the right to health, even though it is included in the chapter of social rights of the Federal Constitution of 1988, can be read as a fundamental right, through an extensive interpretation of the right to life. The hypothesis launched is that extrafiscality appears as a strong stimulus to sustainable practices in waste management, effecting the promotion of the

¹ O presente trabalho foi realizado com apoio do Conselho Nacional de Desenvolvimento Científico e Tecnológico - CNPq.

² Mestranda em Direito pela PUCRS. Membro do Grupo de Pesquisas Avançadas em Direito Tributário (GTAX-PUCRS). Email: victoria.maltchik@acad.pucrs.br.

fundamental right to health, more specifically, it will be investigated in the collective scope.

Keywords: Planetary Health; Fundamental Rights; Extrafiscality; Solid Waste.

INTRODUÇÃO

Em que pese a saúde esteja diretamente vinculada com a vida humana, o direito à saúde passou a ser objeto de tutela constitucional recentemente. No final da década de 80, quando começaram os movimentos populares de redemocratização do país, a população se manifestou e participou na nova política de saúde dos brasileiros (DALLARI, 2009). É verdade que desde 1934 já era mencionado o direito à saúde na Constituição da República dos Estados Unidos do Brasil, promulgada no período constitucional de Getúlio Vargas, mas o tema se restringia à discussão da competência concorrente entre União e os estados-membros para cuidar da saúde (DALLARI, 2009), isto é, não atribuindo o caráter de essencialidade e fundamentalidade que se tem no tempo presente.

Com advento da Constituição Cidadã, em 1988, o direito à saúde está disposto no artigo 6º (BRASIL, 1988), integrando os direitos sociais. Nota-se, por oportuno, que o Poder Constituinte não optou por fazer a inclusão no rol taxativo de direitos fundamentais previsto no artigo 5º da Carta Magna. Todavia, (SARLET, 2021, pp. 91) argumenta ser viável atribuir a qualidade de “fundamental” a determinados direitos sociais, sob a justificativa que eles possam estar vinculados a outros direitos cujo núcleo são considerados fundamentais. Portanto, com a premissa de que o direito à saúde se desdobra de um outro direito fundamental, expresso no *caput* do artigo 5º, qual seja: o direito à vida (BRASIL, 1988), bem como do princípio da dignidade da pessoa humana, ele pode ser compreendido enquanto um direito fundamental.

Ocorre que, algumas ações efetuadas pela sociedade, tanto no âmbito individual quanto coletivo, podem contribuir mais ou menos para a efetivação do direito fundamental à saúde. Ilustrativamente, citam-se o caso do tabagismo e da gestão dos resíduos sólidos urbanos: sabendo dos riscos que a nicotina traz à saúde, os consumidores de cigarros corroboram de forma negativa para promoção da saúde pública, visto que contribuem, mesmo com ciência dos malefícios de suas escolhas

ao restante da população, ocupar do tempo e dos espaços públicos de saúde. De forma semelhante, porém no cenário coletivo, tem-se que a má administração dos resíduos sólidos pelos responsáveis, seja por parte das pessoas que não corroboram com a separação do lixo em suas residências ou pelo órgão de coleta insuficiente em uma região específica, pode acarretar em diversas doenças.

Em ambos os casos o direito tributário pode atuar enquanto *player* no estímulo de condutas mais ou menos desejadas pelo Estado. Assim, o objetivo geral desta investigação é verificar em qual medida a extrafiscalidade auxilia a firmar a cultura de sustentabilidade na coleta e reciclagem de resíduos sólidos urbanos, de modo a afastar as doenças provenientes do mau manejo deles. Por sua vez, os objetivos específicos contam com a elucidação do conceito de extrafiscalidade, bem com a exposição dos incentivos fiscais existentes no Brasil no que tange a administração do lixo. Por derradeiro, relacionar-se-á a eficácia dos programas estudados no contexto de saúde pública.

1 O CONCEITO DE EXTRAFISCALIDADE

O Código Tributário Nacional, instituído pela Lei nº 5.170 de 1966, apresenta as normas gerais de direito tributário aplicáveis à União, Estados e Municípios. A definição de tributo trazido pelo Código é:

Art. 3º Tributo é toda prestação pecuniária compulsória, em moeda ou cujo valor nela se possa exprimir, que não constitua sanção de ato ilícito, instituída em lei e cobrada mediante atividade administrativa plenamente vinculada (BRASIL, 1966).

Antes que se possa adentrar no conceito de extrafiscalidade, é necessário explicar que a tributação tem como objetivo a arrecadação de recursos para manutenção das atividades públicas (BALEEIRO, 2008, p.149). No entanto, o tributo também pode assumir outras finalidades, como ensinam (ATALIBA, 1966), (GONÇALVES, 2016) e (CALIENDO, 2019); os autores referem que a extrafiscalidade atua para além da estritamente financeira, podendo regular a sociedade, economia e

política, estimulando ou desestimulando condutas mais ou menos desejadas quando se almeja alcançar e firmar determinada cultura.

O vocábulo “extrafiscalidade” tem seu conceito melhor elucidado por (BOMFIM, 2014, p. 25):

O prefixo “extra”, portanto, é utilizado para indicar outras funções que podem ser exercidas pela tributação e que não vinculam diretamente à função arrecadatória, o que é absolutamente diferente de considerá-lo como excludente do próprio campo tributário. No contexto em que a expressão é empregada, o vocabulário “fiscalidade” não pode ser tomado como sinônimo de tributação, mas como sinônimo de arrecadação (grifos do autor).

Há doutrinadores, como (ÁVILA, 2009, p. 307), que defendem a influência do direito tributário no comportamento dos contribuintes até mesmo quando a intenção do legislador não seja essa. Isso porque, o simples fato de aumentar ou diminuir a carga tributária sobre algum produto ou serviço já afeta os sujeitos da relação. Em síntese, para (ÁVILA, 2009, p. 307) as normas que possuem caráter fiscal *prima facie* também induzem comportamentos.

Ao que interessa aqui, é compreender que o direito tributário, sobretudo através da extrafiscalidade, pode atuar como relevante ferramenta para reduzir as externalidades negativas, bem como para aumentar as externalidades positivas, as quais são almejadas ao se viver em sociedade harmonicamente. A respeito dos estudos das externalidades, (PIGOU, 1962, p. 192) discorre que a neutralização advém da internalização dos custos produzidos por aqueles que as deram causa. Em outros termos: o Estado interferiria na economia, considerando as externalidades produzidas, sem a elas negativas ou positivas, no cálculo dos tributos.

A crítica que se faz ao pensamento pigouviano é, justamente, reproduzir na prática o valor que cada externalidade representaria. Nesse sentido, (COASE, 1960, p. 25) ataca os defensores das taxas pigouvianas sob a justificativa de que o valor cobrado, de acordo com o idealizado por (PIGOU, 1962), deve ser idêntico ao dano causado, ou seja, o mesmo em relação à externalidade negativa a que se deu

origem. Outro obstáculo, na visão de (COASE, 1960), é o fato do pagamento dos tributos ser destinado ao sujeito, muitas vezes, alheio ao que sofreu o dano, a externalidade negativa.

Esclarece-se, no ponto, esclarecer que muitos dos estudos de (PIGOU, 1962) tiveram como inspiração os danos causados ao meio ambiente e, por isso, as críticas de (COASE, 1960) possuem fundamento; é notório que o pagamento majorado de um tributo em razão de eventual ambiental causado acaba por beneficiar, numa primeira análise, o órgão recebedor do montante. Isso pois, as indenizações, relacionadas ao direito civil, teriam como sujeito recebedor o mesmo que sofreu o prejuízo, diferentemente de como acontece quando da cobrança da externalidade negativa através da tributação.

Independentemente dos óbices encontrados na teoria pigouviana, *mister* salientar as ricas contribuições que o autor entregou à comunidade acadêmica e, conseqüentemente, à sociedade. O nobre doutrinador demonstrou como o direito tributário pode trabalhar com a contenção ou promoção de políticas públicas, que vão desde a manutenção do direito ao meio ambiente ecologicamente equilibrado até o direito à saúde.

Conhecendo a divergência doutrinária acerca do dever fundamental de pagar tributos (NABAIS, 1998, p. 70) e do planejamento tributário (LEÃO, 2018), o que se expõe unicamente com fim dialético, defende-se neste trabalho a ideia de que o direito tributário se trata de um dever fundamental, haja vista os custos pecuniários que os direitos fundamentais contam para garantir a sua efetivação.

2 A RELAÇÃO ENTRE A EXTRAFISCALIDADE E A GESTÃO DOS RESÍDUOS SÓLIDOS

A Lei nº 11.445/2007 conceitua o saneamento básico como um conjunto de serviços, instalações operacionais de abastecimento de água potável, esgotamento sanitário, limpeza urbana e gestão de resíduos sólidos, além da drenagem e do manejo das águas pluviais urbanas (BRASIL, 2007). Considerando que este artigo analisa especificamente o tema dos resíduos sólidos, salienta-se que a Política Nacional de Resíduos Sólidos (PNRS - Lei Federal nº 12.305, de agosto de 2010) é o marco legal da matéria no Brasil. Antes de entrar em vigor, a lei tramitou em várias

instâncias dos poderes Legislativo e Executivo por mais de duas décadas antes que fosse aprovado e promulgado. O lapso temporal fez com que o teor da lei, mesmo depois de promulgada, se demonstrasse defasado, gerando dificuldade para efetivação das metas ali contidas (ZAGO; BARROS, 2019).

Entretanto, conforme melhor abordar-se-á, a PNRS prevê instrumentos que ainda podem atenuar os desafios enfrentados. Anteriormente a isso, possibilitando uma melhor compreensão sobre o cenário brasileiro no setor dos resíduos sólidos, apresentar-se-á os números obtidos nos últimos relatórios. A Associação Brasileira de Empresas de Limpeza Pública e Resíduos Especiais (ABRELPE) publica relatórios anuais, os quais demonstram o resultado de importantes índices para o bom entendimento da administração dos resíduos sólidos no país, como, por exemplo, o volume de lixo produzido em determinado recorte temporal estabelecido, assim como as regiões que mais e menos realizam a coleta seletiva dele.

No ano de 2021 foi constatado que os brasileiros produziram em média 81,8 milhões de toneladas, o que significa 224 mil toneladas diárias e equivale em torno de 1,043 kg de lixo por pessoa ao dia (ALBEPRE, 2022). Outra informação interessante a se apontar é o leve decréscimo aparecido nos números em relação aos anos anteriores. Em parte, como explicado pela (ALBEPRE, 2022), isso se deve ao retorno presencial de algumas atividades que foram interrompidas durante o isolamento social imposto aos cidadãos quando do combate da COVID-19. Resumidamente, o relaxamento das restrições contribuíram na diminuição da produção do lixo residencial, tendo em vista que outros espaços (salas comerciais, restaurantes, parques, *shoppings centers* etc.) voltaram a ser frequentados.

Basta, para a presente investigação, perceber que mesmo com os números um pouco menores, a produção de resíduos sólidos é volumosa pelos brasileiros. Desse modo, o mau descarte deles implica em diversas consequências negativas, externalidades negativas, as quais serão sentidas no âmbito individual, ao se analisar o micro, e coletivo, no contexto macro. Infelizmente, a quantidade de municípios que não conta com programa de coleta seletiva é elevada: em 2021, somente 75,1% dos municípios detinham esse serviço, fazendo com que, logicamente, 24,9% fossem deficitários nessa demanda (ALBEPRE, 2022).

Outro problema a ser enfrentado é a destinação dos resíduos depois de

ocorrida a coleta seletiva, ou seja, não é suficiente apenas separar os materiais por tipos pré-estabelecidos, mas é preciso que seu redirecionamento seja feito a um local que seja seguro em relação à saúde dos cidadãos. Um dos maiores desafios brasileiros, entretanto, transcende a coleta dos resíduos sólidos urbanos, sendo a destinação final um ponto de grande preocupação: não tendo sido viável a reinserção do material no mercado, é feito o encaminhamento dele aos lixões e aterros ainda operam nas regiões do país (ALBREPPE, 2022, pp. 26-27).

Curiosamente, muito disso acontece devido à falta de incentivos fiscais que auxiliem na promoção da efetiva gestão do lixo. O artigo 8º da PNRS estabelece os instrumentos dos quais a Lei se vale para atingir os seus objetivos, estando listado no rol a utilização de incentivos fiscais (BRASIL, 2010). Não obstante, desde 2010, com a entrada em vigor da PNRS, o Brasil enfrenta muita resistência à concessão dos benefícios fiscais nos itens reciclados. A fim de dirimir essa questão, criou-se a Lei de Incentivo à Reciclagem (Lei nº 14.246/2021) em 2021, a qual permite que mais projetos que envolvam a reciclagem possam ser alvo de dedução do Imposto de Renda (IR) (BRASIL, 2021).

Não é apenas no âmbito federal que os incentivos fiscais atuam. Evidentemente, a complexidade de se explorar aqueles relativos à competência estadual e municipal é maior, haja vista o tamanho continental do Brasil. Ilustrativamente, citam-se os casos do Imposto de Circulação de Mercadorias e Serviços (ICMS), imposto de competência estadual, e o Imposto sobre a Propriedade Predial e Territorial Urbana (IPTU), de competência municipal.

O ICMS é regulado constitucionalmente pela Lei Complementar nº 87/1996, tendo como fato gerador situações como: (i) a saída de mercadorias de estabelecimento de contribuinte, mesmo se para outro estabelecimento dele; (ii) o fornecimento de alimentação, bebidas e demais mercadorias por qualquer estabelecimento; e, (iii) o início da prestação de serviços de transporte interestadual e intermunicipal de qualquer natureza (BRASIL, 1996).

Visando auxiliar na adesão da reciclagem, muitos estados brasileiros resolveram diminuir a alíquota do ICMS quando constata atividade que se valesse de insumos e produtos reutilizados. Um exemplo disso, é Tocantins, que desde o final da década de 90, com a Lei nº 1.095, isentou por 25 anos o ICMS relativo às saídas

internas de papelão usado, sucatas de metais, plásticos, vidros e demais resíduos, se o contribuinte fosse cadastrado no Programa Estadual de Coleta Seletiva do Lixo - LIXOBOM (RIBEIRO; QUEIROZ; GRUPENMACHER, 2014, p. 69).

Já o IPTU está previsto nos artigos 156, I, da CF/88 (BRASIL, 1988) e 32 a 34 do CTN (BRASIL, 1966). O fato gerador do IPTU consiste na propriedade, no domínio útil ou na posse do imóvel, o qual deve estar localizado em zona urbana municipal, sendo o contribuinte o sujeito que se enquadrar em qualquer uma dessas hipóteses (BRASIL, 1966). Apesar da definição de zona urbana ser descrita em lei municipal, em virtude da competência do tributo, o CTN traz alguns requisitos mínimos que devem ser observados. Similarmente ao que acontece com o ICMS, muitos municípios começaram com a iniciativa do IPTU Verde, que pretende incentivar práticas de condutas ecológicas nas residências dos brasileiros.

Nessa toada, demonstra-se o caso de Guarulhos; a Lei nº 6.793/2011, da cidade paulista, prevê o desconto de 5% de desconto no IPTU para os contribuintes que efetuarem a separação do lixo corretamente e que destinem a sua coleta para reciclagem e aproveitamento deles (PREFEITURA GUARULHOS, 2011). É inequívoco que isso por si só seja capaz de mudar o rumo de todo tratamento do lixo e, por resultado, de todas as doenças que ele possa transmitir quando exposto às pessoas. Ao mesmo tempo, entende-se que a vantagem econômica torna mais atrativa a ação positiva para os indivíduos, que, aos poucos, passam a firmar tradições de cuidado para com o descarte dos resíduos.

3 EXTRAFISCALIDADE, GESTÃO DE RESÍDUOS SÓLIDOS E SAÚDE PLANETÁRIA

Finalmente, depois de conceituada a extrafiscalidade e traçadas breves comentários acerca do contexto nacional na gestão dos resíduos sólidos, resta relacionar as observações percebidas com a saúde planetária. Destarte, como contextualiza (GOLDIM; FERNANDES, 2021, pp. 59-60), a ideia de saúde planetária substituiu a de saúde global. Embora o termo saúde global já trouxesse relevantes reflexões sobre o caráter multi e interdisciplinar, o cerne seguiu sendo somente o ser humano, enquanto a saúde planetária, sugerida pela *Rockefeller Foundation-Lancet Commission on Planetary Health* no ano de 2015 (GOLDIM; FERNANDES, 2021, pp. 59-

60), perpassa o âmbito do meio ambiente, da saúde coletiva, bem como dos aspectos sociais:

Our definition of planetary health is the achievement of the highest attainable standard of health, wellbeing, and equity worldwide through judicious attention to the human systems—political, economic, and social—that shape the future of humanity and the Earth’s natural systems that define the safe environmental limits within which humanity can flourish. Put simply, planetary health is the health of human civilisation and the state of the natural systems on which it depends³. (Whitmee et al., 2015, p.1978)

A definição deixa esclarecido que a saúde planetária se preocupa para além da saúde individual, mas percorre o mais alto grau de bem-estar aos cidadãos, que, para isso, devem cuidar do ecossistema no qual estão inseridos. Com a devida venia, a crítica que se faz ao conceito do autor, com fins unicamente dialéticos, é sua grande semelhança com o significado de desenvolvimento sustentável, que, por sua vez, também é alvo de discordâncias.

Para atender aos fins pretendidos, o que se precisa saber é a íntima relação existente entre o desenvolvimento sustentável com a economia, a sociedade e o meio ambiente, sendo essa a principal aproximação existente entre os conceitos explorados. Defende-se, porém, que o conceito de saúde planetária foi um marco urgente e imprescindível, pois relaciona, explicitamente, fenômenos complexamente interligados e que tempos atrás foram ignorados:

A proposta de saúde planetária amplia essa abordagem para o planeta, para a biosfera, onde todos os elementos podem ser incluídos e relações, antes não percebidas, passam a ter um importante papel em termos de relações.

³ A nossa definição de saúde planetária é a realização do mais alto padrão alcançável de saúde, bem-estar e equidade a nível mundial através de uma atenção criteriosa aos sistemas humanos - políticos, económicos e sociais - que moldam o futuro da humanidade e dos sistemas naturais da Terra que definem os limites ambientais seguros dentro dos quais a humanidade pode florescer. Em resumo, a saúde planetária é a saúde da civilização humana e o estado dos sistemas naturais dos quais ela depende (tradução própria).

Fenômenos que não são perceptíveis em um dos planos passam a sê-lo em outro. Da mesma forma, a abordagem bioética pode assumir essas diferentes perspectivas. O que seria correto em termos de macroalocação de recursos para um único indivíduo, pode ser equivocado quando o foco se amplia e passam a ser discutidos critérios de macroalocação para uma comunidade (GOLDIM; FERNANDES, 2021, p. 62).

O desenvolvimento sustentável explora diversas áreas, mas, distintamente da saúde planetária, as segmenta em setores tentando, ao final, juntá-los para uma leitura sistemática e interdisciplinar. Não se pretende negar às efetivas abordagens do desenvolvimento sustentável. Pelo contrário: entende-se a sua pertinência no cenário internacional. Entretanto, tem-se que a saúde planetária é um termo que melhor se adequa à pesquisa. Nesse sentido, poder-se-ia adentrar no conceito de meio ambiente ecologicamente equilibrado a fim de argumentar como os recursos naturais estão plenamente vinculados à própria existência humana.

Atualmente, existe uma agenda internacional (Agenda 2030 da Organização das Nações Unidas) em vias de fornecer um maior bem estar social às pessoas. Para isso, medidas em combate à pobreza e à fome foram pensadas, da mesma forma que planos para fornecer acesso à educação de qualidade e melhorar as condições de saneamento básico, entre outros aspectos (WHO, 1978).

Não dispondo de uma conceituação globalmente unânime sobre o termo, seguir-se-á a definição brasileira do que se entende por meio ambiente ecologicamente equilibrado. Conceituado como um bem comum de uso do povo, o meio ambiente ecologicamente equilibrado precisa ser garantido para manter a sadia qualidade de vida das presentes e futuras gerações, sendo esse um princípio norteador do direito ambiental internacional (SARLET; FENSTEREIFER, 2020) (SARLET; FENSTEREIFER, 2021). Como uma comunidade sozinha não consegue garantir todos critérios exigidos na manutenção do meio ambiente sadio, necessita-se do engajamento da comunidade internacional.

Do mesmo modo como proposto por (KANT, 2004), defende-se o planeta Terra enquanto unidade. A discussão ambiental, demanda da participação de todos os cidadãos do globo não se restringindo, então, apenas aos países que optaram por

ratificar tratados internacionais sobre a temática. Por esse motivo, lê-se o direito o meio ambiente ecologicamente equilibrado como um direito cosmopolita, como o último estágio do direito (KANT, 2004).

No âmbito do direito interno, a doutrina se manifesta quanto a eficácia horizontal dos direitos fundamentais, em que coloca os particulares enquanto coobrigados do Poder Público na tutela desses direitos (SARLET, 2021), de maneira controvertida, se afastando, infelizmente, daquilo pensado pelo filósofo alemão. Isso pois há quem defenda o Estado enquanto único guardião e prestador dos direitos fundamentais (DIMOULIS; MARTINS, 2014). Em razão disso, foca-se exclusivamente na atuação do Estado, através da concessão ou não de incentivos fiscais, nos resíduos sólidos e, por corolário lógico, na área da saúde.

Sustentabilidade também é um termo relevante, porque diz respeito à capacidade de criar meios alternativos para suprir as necessidades básicas das presentes e futuras gerações, que costumam ser questões vinculadas à economia, à sociologia, à cultura e ao meio ambiente. Ao contrário do que muitos imaginam, a sustentabilidade abrange mais assuntos do que a proteção ambiental, e, como leciona (FREITAS, 2019, p.125), é:

[...] nada obstante as distintas cargas semânticas, a sustentabilidade (a) é princípio ético-jurídico, direta e imediatamente vinculante (do qual são inferíveis regras-chave), que determina o oferecimento de condições, objetivas e subjetivas, para fruição do bem-estar das atuais e futuras gerações, (b) é valor constitucional supremo (critério axiológico de avaliação dos impactos de condutas públicas e privadas) e (c) é objetivo fundamental da República (norte integrativo da interpretação do Direito) (grifos do autor).

Todavia, o recorte da presente pesquisa se limitou a entender os impactos do mau descarte do lixo na saúde coletiva brasileira. A ausência de saneamento básico em diversas localidades do Brasil, potencializada pelo imprópria gerência dos resíduos sólidos, pode causar impactos diretos na saúde da população. Segundo (ALBEPRE, 2022), o lixo gera poluição da água, flora e fauna, emitindo gás carbônico (CO₂) para atmosfera e essas condições fragiliza a saúde daqueles que residem no

entorno, abrangendo um raio de até 60km (ALBEPRE, 2022).

Quantos às doenças relacionadas ao saneamento ambiental inadequado, (COSTA et al, 2002, p.3) as classifica de acordo com as formas de transmissão, podendo ser elas (i) feco-oral; (ii) inseto vetor; (iii) contato com a água etc. Dentre as principais doenças estão diarreia, cólera, hepatite A, dengue, malária e doença de chagas (COSTA et al, 2002, p.3). Não bastasse isso, o relatório estima que em razão dos aterros e lixões, no período de 2016 a 2021, o “gasto total da saúde no Brasil para tratar dos problemas causados em decorrência da destinação inadequada de resíduos foi de 1,85 bilhão de dólares” (ALBEPRE, 2022, p.34)

Mesmo reconhecendo as diferentes abordagens do direito orçamento e do direito tributário, é percebida a correlatividade entre os ramos. Ao se falar em gastos públicos, como supracitado, é inevitável pensar que contenções podem ser instituídas através da tributação. Isso porque, como aprendido até aqui, a extrafiscalidade corrobora na formação e sustentação de ações que são quistas. Com isso, viu-se que o gerenciamento dos resíduos sólidos também pode ser mais eficaz nas zonas em que se conta com determinada vantagem fiscal. Os incentivos fiscais são fundamentais no setor, porquanto estimulam às práticas de separação do lixo, coleta seletiva e destinação adequada.

Havendo iniciativas minimamente suficientes na administração do lixo, as doenças provenientes de roedores e insetos vetores de doenças são contidas, dando espaço para outras questões a serem superadas na saúde coletiva brasileira, como as consequências da desnutrição causada pela pobreza, estando esses englobados na Agenda 2030. Ratifica-se, ainda, que a saúde planetária visa associar as necessidades humanas com o ecossistema do qual o ser humano faz parte, fazendo com que o cuidado com o apropriado descarte do lixo reflita em positivos efeitos ao meio ambiente.

CONCLUSÕES

O direito à saúde, mesmo sem estar expressamente previsto no rol do artigo 5º da CF/88, é considerado um direito fundamental, estando diretamente vinculado ao direito fundamental à vida e, por isso, deve ser promovido solidariamente pelos

entes federados. Muitos são os obstáculos encontrados na saúde coletiva brasileira, porém, as doenças provenientes do mau manuseio dos resíduos sólidos podem ser contornáveis através de condutas sustentáveis a serem estimuladas pelo Estado.

No decorrer do trabalho, conceitou-se extrafiscalidade, tendo ela finalidade que transcende a mera arrecadação de tributos para financiamento das atividades estatais, isto é, explorou-se a ideia de promoção e manutenção de novas culturas mais e menos desejadas pelos governantes mediante o direito tributário.

Ato contínuo, verificou-se que a má administração do lixo gera impactos negativos (externalidades negativas) à natureza, que, por sua vez, acarreta em proliferação de doenças. Nesse momento, surge um dever fundamental de atenção e promoção na defesa ambiental, justamente para atender às políticas de saúde coletiva, e efetivar o direito fundamental à saúde.

Isso ocorre devido a próxima relação que o meio ambiente ecologicamente equilibrado guarda com a saúde, tendo sido, na oportunidade, elucidou-se o conceito de saúde planetária. Nesse contexto, demonstrou-se as algumas das doenças proferidas pelo lixo, bem como o investimento público necessário para freá-las. Outrossim vislumbra-se que muitas delas podem ser contornadas quando práticas sustentáveis são postas em prática, tais como a separação do lixo, coleta seletiva, reciclagem e destinação apropriada dos resíduos sólidos, já que roedores e demais insetos vetores de doenças não têm espaço no cenário traçado.

Com intuito de encorajar as ações ecológicas pretendidas, viu-se que os incentivos fiscais, previstos no artigo 8º da PNRS, atuam como indutores de comportamentos almejados pelos entes estatais, podendo contribuir para significativas mudanças na sociedade. Diante disso, percorreu-se, ainda que em caráter simplesmente exemplificativo, os benefícios fiscais existentes no setor, mostrando a atratividade na adoção do efetivo manuseio dos resíduos sólidos.

Desse modo, foi demonstrado (i) a saúde enquanto um direito fundamental; (ii) o meio ambiente ecologicamente equilibrado na qualidade de direito-dever fundamental; (iii) a necessária atenção ao saneamento básico, sobretudo aos resíduos sólidos, para manutenção e promoção ao meio ambiente ecologicamente equilibrado e ao direito fundamental à saúde; e, (iv) a extrafiscalidade tributária enquanto player na promoção de condutas desejáveis e, por conseguinte, a no

estímulo de práticas sustentáveis, as quais afastam a proliferação de doenças na população brasileira. Feitas essas considerações, entende-se que o debate é de suma importância para sociedade, haja vista a agenda internacional sobre o tema.

REFERÊNCIAS

ABRELPE. **Panorama dos Resíduos Sólidos no Brasil 2022**. Abrelpe, 2022. Disponível em: <https://abrelpe.org.br/panorama/> Acesso em: 14 jan. 2023.

ATALIBA, G. **Sistema constitucional tributário brasileiro**. São Paulo: Revista dos Tribunais, 1968.

ÁVILA, H. **Segurança jurídica no direito tributário – entre permanência, mudança e realização**. Tese apresentada junto à Universidade de São Paulo. São Paulo, 2009.

BALEEIRO, A. **Uma Introdução à Ciência das Finanças**. 16ª ed. Rio de Janeiro: Forense, 2008.

BOMFIM, D. M. C. **Extrafiscalidade: identificação, fundamentação, limitação e controle**. 2014. Tese (Doutorado em Direito Econômico, Financeiro e Tributário) - Universidade de São Paulo, São Paulo, 2014. Disponível em: < https://teses.usp.br/teses/disponiveis/2/2133/tde-09082017-160000/publico/TESE_COMPLETA_Diego_Marcel_Costa.pdf > Acesso em: 03 jan. 2023.

BRASIL. **Lei nº 5.172 de 25 de outubro de 1966**. Dispõe sobre o Sistema Tributário Nacional e institui normas gerais de direito tributário aplicáveis à União, Estados e Municípios. Disponível em <https://www.planalto.gov.br/ccivil_03/leis/l5172compilado.htm> Acesso em: 12 dez. 2022.

BRASIL. **Constituição da República Federativa do Brasil**. Brasília: Senado Federal, 1988.

BRASIL. **Lei Complementar nº 87 de 13 de setembro de 1996**. Dispõe sobre o imposto dos Estados e do Distrito Federal sobre operações relativas à circulação de mercadorias e sobre prestações de serviços de transporte interestadual e intermunicipal e de comunicação, e dá outras providências. Brasília. Disponível em: < https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp87.htm > Acesso em: 13 dez. 2022.

BRASIL. **Lei nº 11.445 de 05 de janeiro de 2007**. Estabelece as diretrizes nacionais para o saneamento básico. Brasília. Disponível em<

planalto.gov.br/ccivil_03/_ato2007-2010/2007/lei/L11445compilado.htm> Acesso em: 10 dez. 2022.

BRASIL. **Lei nº 12.305 de 02 de agosto de 2010.** Institui a Política Nacional de Resíduos Sólidos; altera a Lei no 9.605, de 12 de fevereiro de 1998; e dá outras providências. Brasília. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2010/lei/l12305.htm > Acesso em: 10 jan. 2022.

CALIENDO, P. **Curso de Direito Tributário.** São Paulo: Saraiva Educação, 2019.

COASE, R. H. **The problem of social cost.** Journal of law and economics: Chicago, 1960.

COSTA, A. M.; PONTES, C. A. A.; MELO, C. H.; LUCENA, R. C. B.; GONÇALVES, F. R.; GALINDO, E. F. **Classificação de doenças relacionadas a um saneamento ambiental inadequado (DRSAI) e os Sistemas de Informações em Saúde no Brasil:** possibilidades e limitações de análise epidemiológica em saúde ambiental. In: CONGRESSO INTERAMERICANO DE INGENIERIA SANITARIA Y AMBIENTAL, 28., 2002, Cancun. Proceedings. Cancun: Asociacion Interamerican de Ingenieria Sanitaria y Ambiental: ABES, 2002. 1 CD-ROM.

DALLARI, S. G. **A construção do direito à saúde no Brasil.** São Paulo: Revista de Direito Sanitário, 2009.

DIMOULIS, D.; MARTINS, L. **Teoria Geral dos direitos fundamentais.** São Paulo: Atlas, 2014.

FREITAS, J. **A interpretação sistemática do direito.** Belo Horizonte: Fórum, 2019.

GOLDIM; J. R; FERNANDES, M. S. **Os novos contextos da disseminação de doenças: as alterações climáticas e a deslocalização de doenças endêmicas.** Cad. Ibero Am. Direito Sanit. 24º de junho de 2021. Disponível em: <<https://www.cadernos.prodisa.fiocruz.br/index.php/cadernos/article/view/779> > Acesso em: 08 jan. 2023.

GONÇALVES, O. O. **A extrafiscalidade como instrumento para incentivar a produção de energia renovável.** In: CALIENDO, P.; CAVALCANTE, D. L. (Org.). Tributação ambiental e energias renováveis. Porto Alegre: Fi, 2016. pp. 74-98. Disponível em < https://www.editorafi.org/_files/ugd/48d206_c56b50a8c23e461686b9a8419b201244.pdf > Acesso em: 05 jan. 2023.

KANT, I. **Fundamentação da Metafísica dos Costumes.** Trad. Paulo Quintela. Lisboa: Edições 70, 1995.

LEÃO, M. T. **O direito fundamental de economizar tributos:** entre legalidade, liberdade e solidariedade. São Paulo: Malheiros, 2018.

NABAIS, J. C. **O dever fundamental de pagar impostos**. Coimbra: Almedina, 1998.

PIGOU, A. C. **The economics of welfare**. Springfield: Cosimo Classics, 2006.

PREFEITURA GUARULHOS. **Lei nº 6.793 de 28 de dezembro de 2010**. Dispõe sobre o lançamento, arrecadação e fiscalização do Imposto Sobre a Propriedade Predial e Territorial Urbana - IPTU e dá outras providências. Disponível em <https://leis.guarulhos.sp.gov.br/06_prefeitura/leis/leis_download/06793lei.pdf> Acesso em: 03 jan. 2023.

RIBEIRO, M. F.; QUEIROZ, M. E.; GRUPENMACHER, B. T. **Incentivos fiscais e sustentabilidade financeira para a execução de planos municipais de gestão integrada de resíduos sólidos**. In: CAVALCANTE; D. L. (Coord.). Tributação ambiental: reflexos na Política Nacional de Resíduos Sólidos. Curitiba: Editora CRV, 2014. pp. 59-76.

SARLET, I. W. **A eficácia dos direitos fundamentais: uma teoria geral dos direitos fundamentais na perspectiva constitucional**. Porto Alegre: Livraria do Advogado, 2021.

SARLET, I. W.; FENSTEREIFER, T. **Curso de Direito Ambiental**. Rio de Janeiro: Forense, 2020.

_____. **Direito Constitucional Ecológico**. São Paulo: Thomson Reuters Brasil, 2021.

WHITMEE, S. et al. **Safeguarding human health in the Anthropocene epoch: report of the Rockefeller Foundation-Lancet Commission on planetary health**. The Lancet, v.386, 14 nov. 2015. pp.1973-2028.

World Health Organization (WHO). **Declaration of Alma - Ata - International Conference on Primary Health Care**. Alma - Ata: WHO, 1978.

ZAGO, V. C. P.; BARROS, R. T. V.. **Gestão dos resíduos sólidos orgânicos Urbanos no Brasil? Do ordenamento jurídico à realidade**. Engenharia Sanitária e Ambiental, v. 24, 2019. pp. 219-228. Disponível em: < <https://www.scielo.br/j/esa/a/MY53xbTzPxYhz783xdmKc8F/?lang=pt> > Acesso em: 13. dez. 2022.

