UNIVERSIDADE FEDERAL DA BAHIA
FACULDADE DE DIREITO
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO – PPGD
MESTRADO EM DIREITO

KARINA DA HORA FARIAS

IMPACTOS DOS CRIMES CIBERNÉTICOS E OS RISCOS DA INTELIGÊNCIA ARTIFICIAL: OS PILARES DO DIREITO NA PROTEÇÃO DOS DADOS SENSÍVEIS

Salvador
2022

KARINA DA HORA FARIAS

IMPACTOS DOS CRIMES CIBERNÉTICOS E OS RISCOS DA INTELIGÊNCIA ARTIFICIAL: OS PILARES DO DIREITO NA PROTEÇÃO DOS DADOS SENSÍVEIS

Dissertação apresentada ao Mestrado em Direito do Programa de Pós Graduação da Faculdade de Direito, da Universidade Federal da Bahia - UFBA, como requisito obrigatório para obtenção do grau de Mestre.

Área de Concentração: Direitos Fundamentais e Justiça

Linha 4 - Direito Pós-moderno: bioética, cibernética, ecologia e direito animal.

Orientador: Professor-Doutor Salvador Morales Ferrer

Salvador
2022

Dados internacionais de Catalogação na Publicação (CIP)

F224 Farias, Karina da Hora

Impactos dos crimes cibernéticos e os riscos da inteligência artificial: os pilares do direito na proteção dos dados sensíveis / Karina da Hora Farias. – 2022.

167 f. : il., color. ; 30 cm.

Orientador: Prof. Dr. Salvador Morales Ferrer.

Dissertação (Mestrado) – Universidade Federal da Bahia, Faculdade de Direito, Salvador, 2022.

1. Proteção de dados. 2. Inteligência artificial. 3. Cibercrime. 4. Tecnologia e direito. 5. Proteção de dados - Inovação tecnológica. I. Morales Ferrer, Salvador. II. Universidade Federal da Bahia - Faculdade de Direito. III. Título.

CDD – 342.0858

Biblioteca Teixeira de Freitas, Faculdade de Direito, Universidade Federal da Bahia

TERMO DE APROVAÇÃO

KARINA DA HORA FARIAS

IMPACTOS DOS CRIMES CIBERNÉTICOS E OS RISCOS DA INTELIGÊNCIA ARTIFICIAL: OS PILARES DO DIREITO NA PROTEÇÃO DOS DADOS SENSÍVEIS

Dissertação apresentada ao Programa de Pós-graduação da Faculdade de Direito da Universidade Federal da Bahia (PPGD/UFBA), como requisito para obtenção do grau de Mestre em Direito.

Aprovada em 20 de dezembro de 2022. Nota: 10,0 (Dez).

BANCA EXAMINADORA:

Salvador Morales Ferrer – Orientador_____

Doutor em Estudos Jurídicos pela Universitat de València / Espanha

Professor Colaborador - Universidade Federal da Bahia (UFBA)

Dirley da Cunha Júnior _ _____

Pós-Doutor em Direito Constitucional pela Universidade de Lisboa / Portugal

Professor Permanente - Universidade Federal da Bahia (UFBA)

Felipe Rodrigues Bomfim_____

Pós-Doutor em Direito pela Universidade Federal da Bahia / Brasil

Professor Adjunto - Universidade Estadual da Bahia (UNEB)

AGRADECIMENTOS

À Deus, por me demonstrar presença quando ousei duvidar;

Aos Professores Universitários pelo plantio de *sementes vigorosas*;

Aos colaboradores da Universidade, Professores Júlio Rocha, Daniel Oitaven,
e a Técnica Gemimma da Silva, sustentáculos de todos os dias;

Ao Professor Salvador Morales Ferrer pelo mágico acolhimento como orientador,
e à Professora Marta Gimenéz, pelo início da caminhada.

Aos Professores Ramon Suarez Xavier (Universidade de Málaga, Espanha) e Felipe Bomfim (Universidade do Estado da Bahia, Brasil), pela solidariedade acadêmica, além dos muros de suas universidades;

Aos colegas mestrandos e doutorandos de quem tanto recebi academicamente,
um carinho especial a Adriana Cutrim, Larissa Oliveira, Emílio Britto, Jaqueline San Galo, Vinícius Quaresma e Gerson Conceição, significativos encontros para a vida;

À família, Roby, irmãos, amigos, colegas de profissão, por abdicarem da minha presença física, vibrando por cada pequena vitória;

À minha querida mãe que encolheu a dor da solidão por acreditar em tudo que faço, além de me ensinar, a não desistir dos projetos da vida;

À todos, meu imenso, intenso e respeitoso amor.
Não é possível se construir sozinho!

“O direito não constitui um simples conceito –
é uma força viva.

Eis a razão por que vemos a justiça segurando em uma das mãos a balança, por meio da qual o direito é pesado, e na outra a espada, por meio da qual o direito é defendido.

A espada sem a balança é força bruta, ao passo que a balança sem a espada é a impotência do direito.”

Rudolf Von Ihering (2019, p.25)

DA HORA Farias, Karina. **Impactos dos crimes cibernéticos e os riscos da inteligência artificial: os pilares do direito na proteção dos dados sensíveis.** (Dissertação) Mestrado em Direito do Programa de Pós-graduação da Universidade Federal da Bahia (UFBA), Salvador - Brasil, 2022. 167p**.**

RESUMO

Esta dissertação é fruto de pesquisa realizada no Mestrado em Direito da Universidade Federal da Bahia e teve por objeto análise da proteção dos dados sensíveis da população sob o princípio da dignidade da pessoa humana. Objetivou analisar as vulnerabilidades insurgentes com o incremento dos crimes cibernéticos e da inteligência artificial, na dinâmica deste recém-nascido século XXI. Tais vulnerabilidades conduziram ao questionamento sobre quais pilares devem ser considerados na construção do direito, para a proteção de dados sensíveis e humanidade das pessoas, diante dos impactos dos crimes cibernéticos e riscos da inteligência artificial. Para responder tal premissa, o trabalho estruturou-se em cinco partes, apresentando na introdução os aspectos metodológicos e a relevância de empoderar a sociedade, instrumentalizada pelo conhecimento sobre as inovações tecnológicas; no primeiro capítulo, teceu sobre a vulnerabilidade e ressignificação dos dados sensíveis como objeto de valor econômico, diante da revolução tecnológica que conduz a superconectividade digital; no segundo capítulo, foram enaltecidos os fundamentos do direito constitucional à proteção de dados sensíveis e direito à privacidade, sob a teoria do neoconstitucionalismo, visando melhor compreensão do caráter *prima facie* do princípio da dignidade da pessoa humana; no terceiro capítulo, explanou-se sobre os impactos dos crimes cibernéticos no plano nacional e global; no quarto capítulo, foram apresentados os principais riscos da inteligência artificial para os dados sensíveis e humanidade das pessoas, refletindo a necessidade de regulação eficaz; e no quinto capítulo, eclodiu a reflexão sobre os pilares éticos, antidiscriminatórios e humanitários a serem considerados na formação do Direito, para regular as novas tecnologias. Por fim, considerou-se imprescindível a criação de diretrizes éticas, multiculturais e técnicas robustas sobre inteligência artificial, com investimentos em pesquisa e criação de observatório técnico permanente, que possibilite o desenvolvimento inclusivo e humanitário dessas inovações, submetidas de modo vinculado, à máxima expressão de tutela social.

Palavras-Chave: proteção de dados; inteligência artificial; crime cibernético; direito digital; inovação tecnológica.

DA HORA Farias, Karina. **Impacts of cyber crimes and the risks of artificial intelligence: the pillars of law in the protection of sensitive data**. (Dissertation) Master's Degree in Law from the Graduate Program of the Federal University of Bahia (UFBA), Salvador - Brazil, 2022. 167p.

ABSTRACT

This dissertation is the result of research carried out in the Master's Degree in Law at the Federal University of Bahia and aimed to analyze the protection of sensitive data of the population under the principle of human dignity. It aimed to analyze insurgent vulnerabilities with the increase in cybercrime and artificial intelligence, in the dynamics of this newborn 21st century. Such vulnerabilities led to the questioning of which pillars should be considered in the construction of law, for the protection of sensitive data and people's humanity, in the face of the impacts of cybercrime and risks of artificial intelligence. To answer this premise, the work was structured in five parts, presenting in the introduction the methodological aspects and the relevance of empowering society, instrumentalized by knowledge about technological innovations; in the first chapter, he wove about the vulnerability and resignification of sensitive data as an object of economic value, in the face of the technological revolution that leads to digital superconnectivity; in the second chapter, the fundamentals of the constitutional right to the protection of sensitive data and the right to privacy were praised, under the theory of neoconstitutionalism, aiming at a better understanding of the prima facie character of the principle of human dignity; in the third chapter, the impacts of cyber crimes at the national and global level were explained; in the fourth chapter, the main risks of artificial intelligence for sensitive data and people's humanity were presented, reflecting the need for effective regulation; and in the fifth chapter, reflection on the ethical, anti-discriminatory and humanitarian pillars to be considered in the formation of Law, to regulate new technologies. Finally, it was considered essential to create ethical, multicultural and robust technical guidelines on artificial intelligence, with investments in research and the creation of a permanent technical observatory, which enables the inclusive and humanitarian development of these innovations, submitted in a linked manner, to the maximum expression of social protection.

Key-words: data protection; artificial intelligence; cyber crime; digital law; technologic innovation.

LISTA DE GRÁFICOS

LISTA DE IMAGENS

LISTA DE SIGLAS

ANPD	Autoridade Nacional de Proteção de Dados
BID	Banco Interamericano de Desenvolvimento
BSI	Bundesamt für Sicherheit in der Informationstechnik
CEDH	Comissão Europeia dos Direitos do Homem
CERT.br	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
CETIC.br	Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação
CGI	Comitê Gestor de Internet
CNJ	Conselho Nacional de Justiça
CRFB	Constituição da República Federativa do Brasil
C.SIRT	Centro de estudo, resposta e tratamento de incidentes
DUDH	Declaração Universal de Direitos Humanos
EC	Emenda Constitucional
ECA	Estatuto da Criança e do Adolescente
E-CIBER	Estratégia Nacional de Segurança Cibernética
ESG	Environmental, Social and Governance
ESPIN	Emergência em Saúde Pública de Importância Nacional
EUA	Estados Unidos da América
INTERPOL	Organização Internacional da Polícia Criminal
ISO	International Organization for Standardization
LGPD	Lei Geral de Proteção de Dados
FBI	Federal Bureau Investigation
FEM	Fundo Econômico Mundial
FGV	Fundação Getúlio Vargas
OCDE	Organização para a Cooperação e Desenvolvimento Econômico
OMS	Organização Mundial de Saúde
ONU	Organização das Nações Unidas
PL	Projeto de Lei
RGPD	Regulamento Geral de Proteção de Dados
SBDC	Sistema Brasileiro de Defesa Cibernética
STF	Superior Tribunal Federal
TJ	Tribunal de Justiça
TSE	Tribunal Superior Eleitoral
TPI	Tribunal Penal Internacional
EU	União Europeia
UEA	Emirados Árabes Unidos
UNESCO	Organização das Nações Unidas para a Educação, a Ciência e a Cultura
UFBA	Universidade Federal da Bahia
USA	Estados Unidos da América

US$	Dólar - Valor em Dólar americano
R$	Real - Valor em Real brasileiro

GLOSSÁRIO

Algorítmo: uma sequência de procedimentos que busca realizar uma tarefa, a partir da solução de um problema lógico ou matemático, bem como, correlacionando dados;

Big Data: tecnologia que possibilita manipular grande quantidade de dados;

Big Tech: grande empresa que domina o mercado da tecnologia da informação;

Ciberespaço: espaço não físico, computacional, cibernético ou virtual;

Cibernética: estudos conjuntos da comunicação e eletrônica, atual ciência da informação;

Cibercriminoso: delinquentes que atuam no ambiente cibernético ou virtual;

Cibersegurança: técnicas para proteção de sistemas informáticos, segurança cibernética;

Criptografia: Técnica de embaralhamento e codificação de dados, que pode ser entendida e decodificada apenas por quem possui uma chave específica;

Cloud Computing: Computação em nuvem;

Cyborgs: é um organismo dotado de partes orgânicas (como o ser humano) e mecânicas (como um robô); é tema difundido pela cibercultura que objetiva ampliar as capacidades do ser orgânico através da tecnologia artificial. Provém das palavras *cyber* (netics) e *organism*, "organismo cibernético" e foi criada por Manfred E. Clynes e Nathan S. Kline (1960), quando se referiram a melhorias no ser humano para sua sobrevivência no espaço cibernético.

E-commerce: Comércio digital;

Hardware: Parte física (dura, palpável) dos computadores;

IA: Inteligência Artificial – tecnologia computacional de alto nível criada para que a máquina aprenda tarefas inerentes aos seres humanos, como o raciocínio.

Indústria 4.0: também denominada quarta revolução industrial, caracterizada pela evolução das tecnologias robóticas e da inteligência artificial, algorítimos, entre outras;

Iot: internet das coisas; equipamentos domésticos ligados à internet;

Live: ambiente de aulas e palestras remoto pela internet, podendo ser ao vivo ou gravado;

Lock Down: fechamento total de espaços públicos e privados;

Phishing: páginas falsas da internet;

Ransomware: programa malicioso informático usado para sequestrar dados de usuários;

Smartificação: uso de smartphones (telefones modernos), utilizados para acesso a internet e realização de tarefas diversas do cotidiano;

Software: programas de computador, uma sequência de instruções a serem seguidas ou executadas pelo computador, construídos para responder a certos estímulos de uso;

Malware: programas maliciosos, usados para cooptar dados e cometer fraudes;

Virtual: ambiente cibernético criado na rede mundial de computadores, mas fisicamente inexistente, criado por programas de computador, que parece ser real aos sentidos.

SUMÁRIO

INTRODUÇÃO

A contemporaneidade é caracterizada pela maior rapidez na comunicação, acesso à informação e inegável interação social, apresentando grande interconectividade entre tecnologias computacionais e redução das distâncias geográficas por meio da rede mundial de computadores, trazendo vantagens antes inimagináveis a sociedade, mas que apresenta, também, desafios a serem superados diante dos novos meios de produção do conhecimento, da economia e das relações de poder que ocorrem no âmbito dessa sociedade em rede, em especial, diante do ordenamento jurídico que precisa se adaptar a esta nova realidade.

A transformação no relacionamento individual e coletivo atual tem como pano de fundo um novo ecossistema baseado no ambiente digital[1], que migrou dos estudos sobre cibernética à contemporânea inteligência artificial, apresentando avanços computacionais mais *inteligentes*, capazes de *aprender*, formatando novos modelos de interação social.

Assim, esta *era da informação*, se apresenta como uma nova *revolução tecnológica* segundo Manuel Castells (2013), ou mesmo, *revolução industrial* "4.0" retratada por Klaus Schwab (2019), este momento apresenta pontos positivos ligados ao desenvolvimento de bens e serviços em um novo ecossistema digital, antes nunca imaginável.

Apesar dos benefícios, parte dessa tecnologia tem vulnerabilizado a dignidade das pessoas e o próprio direito a humanidade, seja pela afetação dos dados sensíveis ou a partir de novos padrões de produção do conhecimento e de manutenção do *poder* inerente ao acesso a informações privilegiadas, trazendo prejuízos importantes a sociedade.

Um exemplo disto é o âmbito penal, no qual os altos índices de criminalidade no espaço digital demonstram que um novo *modus operandi* se instaurou, trazendo consigo a figura dos criminosos cibernéticos e uma nova ordem criminosa diferente da tradicional.

Na mesma direção, os recursos de inteligência artificial resultaram em um levante de benesses em áreas como a medicina, transporte, serviços públicos, serviços assistenciais, etc., fomentando a percepção de que só existem benefícios a serem contabilizados, contudo, tal premissa não se constitui realidade e muito há a observar, além do que apresenta.

Ademais, como acrescenta Castells (2013), existem concepções de poder que envolvem essa era da informação, no qual o *poder em rede* pode ser perigoso ao trazer consigo o uso de novos códigos culturais, dinamismo e flexibilidade, além da forte dualidade entre

[1]Atualmente este ambiente digital é designado como "*information space"*, conceitualmente equivalente a um ambiente ou ecossistema de informação.

conexão e desconexão recaindo na discussão sobre inclusão digital; há também, violações a dignidade humana em prol de projetos hegemônicos que precisam ser ponderados a partir de tais códigos, logo, conhecê-los torna-se elementar.

Apresenta-se justamente aí, na esfera do conhecimento, a relevância deste trabalho científico pelo caráter exploratório que este estudo possui, diante da escassa literatura no Brasil, devendo ser considerada de modo interdisciplinar e transversal, interrelacionando a proteção de dados, crimes cibernéticos e as tecnologias de Inteligência Artificial, a partir das visões do Direito Constitucional, Direito Penal, Direito Civil, Direito à Propriedade Intelectual, Direito Humanitário e Direito Digital, dado o caráter multidisciplinar da temática.

Do ponto de vista acadêmico, o estudo objetiva contribuir para a melhoria do ordenamento jurídico e evolução do Direito para estabelecer boas práticas regulatórias de Inteligência Artificial, como também, servir a sociedade civil como instrumento de poder para melhor compreender os pontos positivos e os riscos da IA, instrumentalizando-a para uma participação proativa e tecnicamente mais qualificada na construção de freios e contrapesos.

É de bom alvitre reforçar que neste momento no âmbito jurídico, o Direito vem sendo criticado quanto à sua obsolência, lentidão e insuficiência em estabelecer eficazes modelos de prevenção, repressão e regulação da Inteligência artificial, diante da violabilidade civil na falha da tutela da proteção de dados e da humanidade das pessoas.

Portanto, tornou-se inevitável questionar sobre quais os principais pilares que devem ser considerados na reconstrução do Direito, de modo a mitigar a ocorrência dos crimes cibernéticos e os riscos da inteligência artificial, visando proteger a população.

Para responder tal problemática, metodologicamente, o caminho escolhido foi o da pesquisa qualitativa, bibliográfica e descritiva, através de pesquisa documental em obras científicas nacionais e estrangeiras como livros, artigos, periódicos, revistas, pesquisas técnicas, monografias, teses, leis e jornais (muitos permeados pelo meio eletrônico), com acesso a documentos primários e secundários, para análise do tema.

Porém, há que ressaltar que a pesquisa teve o método de estudo readaptado durante a sua execução, em razão da sociedade ter sido surpreendida pelo fenômeno da Pandemia ocasionada pelo vírus Sars Covid-19, e o respectivo distanciamento preventivo decretado pelo ente governamental, que impossibilitou o acesso presencial às bibliotecas nacionais e a coleta de dados por interação pessoal, evento superado estrategicamente ao longo da pesquisa.

Como elemento de superação que pode servir de guia em experiência futuras, a adaptação do estudo para o ambiente digital tornou-se imprescindível e ressignificou todo o trabalho de pesquisa, posto que se deu através do monitoramento na internet, das organizações,

universidades e professores que tratavam da temática, com relevância, e de modo obrigatório, por meio da coleta de dados e conhecimento científico através da rede mundial de computadores, visto que a coleta presencial não era indicada.

A pesquisa ocorreu a partir de grupos de discussão virtuais, *ágoras* geograficamente distantes (e a nível global), com produção do conhecimento em encontros remotos, acessos a artigos científicos, periódicos e livros, em sua maioria, digitais.

Como ponto positivo foi realizado acompanhamento da produção científica de especialistas renomados no tema de IA e cibercrimes, participação *sem custos*, em congressos, webinares e palestras síncronas e assíncronas por meio da *web*[2]*;* revertendo o método que sofreu com o distanciamento físico, em elemento favorável, a partir da ampliação da produção acadêmica em termos de qualidade, visto que muitos especialistas e produções não eram acessíveis geograficamente no Brasil, mesmo antes da pandemia.

Como condição *sine qua non*, foi dada maior importância aos canais formais de comunicação científica, capazes de estabelecer "*memória e difusão de informações ao público em geral*" (SILVA e MENEZES, 2005), fundando o trabalho em conhecimentos gerados em processos controlados por organizações sérias de pesquisa.

Ademais, sem desconsiderar de modo cauteloso, informações latentes sobre abusos na proteção de dados e IA que surgiram em meio a velocidade de informações e digitalização mundial das relações, ocorridas justamente durante o período intrapandêmico.

Para fins de diferenciação do modelo de construção formal realizado, revelam as professoras Silva e Menezes (2005, p.14), que a informação não-científica ou informal é aquela que se dá por meio de conversas, contatos pessoais, correspondência e são invisíveis ao público; enquanto que a informação científica formal, encontra-se representada pelos artigos de periódicos, livros, produção de conhecimento construído a partir de estudos sérios.

Na mesma direção estas estudiosas informam que a *avaliação antecipada* realizada por organizações de controle da produção do conhecimento (universidades, laboratórios de pesquisa, empresas, organizações da sociedade civil, etc.) atua de modo preventivo no plano ético metodológico e contribui de duas formas para a certeza da produção científica formal. (SILVA e MENEZES, 2005)

Além de *produzir conhecimento* cientifico por meio de canais oficiais, promove também, a *publicização do conhecimento qualificado*, de modo permanente e com suporte

[2] Refere-se ao termo *world wide web* e sigla *"www"* (rede mundial de computadores), inventados por Tim Berners-Lee em 1955, contudo, somente criou o primeiro *navegador de internet* do mundo, na Suíça em 1989, quando trabalhava para uma organização europeia em pesquisa nuclear.

institucional, tornando-se, portanto, mais acessível a todos (SILVA e MENEZES, 2005); além de evitar a construção de vieses no conhecimento, viciado, pautado em generalizações, ou fomentando estereótipos discriminatórios diversos.

Permeando esta cautela científica, este trabalho foi estruturado em cinco capítulos para compreensão do fenômeno estudado, sendo que no primeiro capítulo abordou-se sobre a evolução da cibernética, a ressignificação dos dados sensíveis como objeto de valor econômico e sua vulnerabilidade diante da superconectividade digital sob influência do fenômeno da pandemia[3], e do consequente, distanciamento físico que lhe sucedera.

No segundo capítulo, discutiu-se sobre aspectos da Constituição Federal do Brasil (1988), enaltecendo os direitos fundamentais à proteção de dados sensíveis e à privacidade, a partir da Teoria do Neoconstitucionalismo, promovendo a análise a partir do caráter *prima-facie* do princípio da dignidade da pessoa humana, como foco nos anseios da sociedade.

No capítulo terceiro, tratou-se dos elementos conceituais e a dinâmica dos crimes cibernéticos e da vulnerabilização dos dados sensíveis que promove nova dinâmica criminosa, diferenciando-a do modelo tradicional, demonstrando seus impactos econômicos e sociais.

No quarto capítulo, foram abordados os principais riscos que o uso indiscriminado da inteligência artificial pode acarretar à sociedade, com potencial para violar os dados sensíveis da população, fragilizar a privacidade e comprometer a inviolabilidade civil, inclusive, com potencial para ferir pressupostos consolidados de proteção humanitária.

No quinto capítulo, foram apresentados os resultados encontrados quanto aos pilares jusfundamentais do Direito, conteúdo filosófico mínimo apto a direcionar as discussões sobre regulação da inteligência artificial, a saber: pilares éticos, antidiscriminatórios e humanitários para o ordenamento jurídico, com foco na proteção da dignidade humana.

Por fim, nas considerações finais, sugeriu-se a criação de normativa brasileira que englobe diretrizes éticas e técnicas robustas sobre Inteligência Artificial, racionalizada a partir da mensuração de riscos e impactos, comportando ações preventivas de controle e expressa negação da tecnologia para projetos de biopoder e discriminação racial, contudo, fomentando o desenvolvimento das boas práticas, e inclusivas, que venham a favorecer a coletividade.

1. VULNERABILIDADE DOS DADOS NO SÉCULO XXI: EVOLUÇAO CIBERNÉTICA E SUPERCONECTIVIDADE PANDÊMICA

[3] Pandemia é termo que tem origem na Grécia "*Pan-demos*" (todo o povo) e, se refere a uma doença infecciosa que alcança simultaneamente diversos indivíduos, em proporção geograficamente global. Disponível em: https://it.wikipedia.org/wiki/Pandemia. Acesso em 22 Abr 2022.

Como retrata Klaus Schwab (2019), a sociedade está vivenciando exatamente neste momento histórico, o que ele denomina de revolução industrial "4.0", tal nível de especialização que fez surgir os estudos sobre a robótica, algorítimos e inteligência artificial, tendo ampliado as possibilidades das máquinas de captarem e processarem dados pessoais sensíveis[4] da população, apresentando tantos benefícios, quanto maléficos à sociedade.

No relato histórico das revoluções tecnológicas, Ramírez (2019) relata que, as revoluções tecnológicas ditam o ritmo do desenvolvimento econômico dos países, impactando no capitalismo cognitivo; este por sua vez, aparelha transformações que produzem novas revoluções tecnológicas, significando modificações na produção do conhecimento, em suas diversas tipologias, conhecimento científico, tecnológico, cotidiano e tradicional.

Para compreender o significado deste século XXI, das transformações no modo de vida das pessoas com o incremento do digital e do virtual que vem ocorrendo, se faz necessário compreender o processo evolutivo das revoluções tecnológicas visando observar o estágio atual da sociedade ocidental.

Há a necessidade de encontrar estratégias seguras de desenvolvimento econômico e social diante das tecnologias da comunicação e informação, lastreadas pelo Direito e, por consequência, pautado na proteção incondicional do princípio da dignidade da pessoa humana e dos direitos fundamentais relevantes, conquistados a duras penas pela sociedade.

Assim, segundo Ramírez (2019), o histórico da primeira revolução tecnológica abarcado entre 1760 a 1840 (segundo alguns estudiosos), ou ocorrido entre o final do século XVI e XVII, trouxe a invenção do motor a vapor como evento significativo, tendo possibilitado a mecanização do trabalho que antes era totalmente manual; a mecanização das tarefas e construção de ferrovias permitiu a comunicação e translado de pessoas e bens.

Nas revoluções seguintes a sociedade experimentou uma ampliação dos sistemas tecnológicos iniciais, ficando marcado entre o final do século XIX e início do XX, a segunda revolução tecnológica (ou industrial), as inovações relacionadas a transportes, fomento a eletricidade, a produção em série e o desenvolvimento da indústria química e siderúrgica; no âmbito da comunicação. As iniciativas do italiano *Marconi* ao inventar a telefonia sem fio com

[4] Dados pessoais sensíveis são informações 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",* das pessoas, conforme o art. 5º da Lei Geral de Proteção de Dados (LGPD); o artigo 12, §2º da mesma lei, informa que o "perfil comportamental" também é considerado dados pessoais para os fins desta lei. (BRASIL, 2018)

a ideia de comunicação em uma espécie de *aldeia global*, revolucionaria definitivamente a sociedade, a partir de então. (RAMÍREZ, 2019).

A terceira revolução iniciada em 1960, segundo Ramírez (2019), então dominada pelos estudos da computação, comunicação, telemática, biotecnologia e a manipulação genética, além de semicondutores, favoreceram a aplicação da internet e levou a construção de recursos cibernéticos a uma escala ainda maior de pessoas.

Nessa direção, considerada como *Quarta Revolução Tecnológica* segundo Ramírez (2019) ou *Indústria 4.0* como reforça Schwab (2019), culmina em diversas técnicas de inteligência artificial, desde a realização de tarefas antes realizadas somente pelos seres humanos, além de criação de aeronaves autodirigíveis e automóveis autônomos, impressão de objetos em terceira dimensão, robotização de tarefas com raciocínio lógico-matemático, emprego de nanotecnologia[5] no cérebro, dados armazenados *em nuvem,* etc.; favorecendo a manipulação de dados.

A criação das e tecnologias de manipulação de grande quantidade de dados, além, da dinâmica dos *e* uso de algorítmos matemáticos, favorecem as manipulações de dados sensíveis pelo âmbito digital. Assim, o dinamismo e a intensidade com que as transformações estão ocorrendo, vem sendo um diferencial importante em relação às demais revoluções anteriores, a velocidade de tais tecnologias no conhecimento, tem sido significativo. (RAMÍREZ, 2019)

Esta nova acepção da quarta revolução tecnológica sobre as coisas, relações sociais que acarreta e funcionalidade das tarefas do cotidiano transformou a sociedade do final do século XX e início deste século XXI e está exatamente neste momento, remodelado a forma de viver das pessoas, de como se relacionam socialmente, como absorvem e externam os institutos do direito individual e coletivo.

E apesar das tecnologias deste momento apresentarem maravilhas do ponto de vista do acesso a informação e a comunicação, em tempo real e de modo global, tais recursos cada vez mais acessível à população de massa, trazem também, possibilidades de fragilização da estrutura dos Direitos Humanos já consolidadas.

Com atenção especial, na estrutura de direitos humanos e fundamentais construídos após a Segunda Guerra Mundial (1945) e as atrocidades que o mundo experimentou, com o

[5] Nanotecnologia são tecnologias que possuem medidas de porte nanomêtrico, objetos que possuem tamanho em escala molecular e atômica entre 1 e 100 nanômetros, sendo que 1 nanômetro equivale a 1 bilionésimo de metro, escala minúscula quando comparada às unidades de medidas que se pode enxergar sem microscópio. Disponível em https://materiaisjr.com.br/tudo-sobre-nanotecnologia/. Acesso em 12 Nov.2022.

abrupto desrespeito a vida e ao direito humanitário global naquele período. Experiência que leva a racionalizar a necessidade de desenvolvimento das tecnologias para a proteção de direitos sensíveis da sociedade e, não, para sua fragilização.

1.1 DADOS, INFORMAÇÕES E O AMBIENTE DE INTERNET

A rede mundial de computadores tornou-se local de compartilhamento de dados e informações, estabelecendo-se como meio de resolução de problemas do cotidiano, tendo se estabelecido e evoluído para um ambiente de interconexão mundial através de uma rede eletrônica de comunicação, que apresenta vantagens e desvantagens inerentes à segurança dos dados sensíveis da população, tornando-se fenômeno desafiador neste início de século XXI.

A *internet*, termo concebido por Vinton Cerf, Yogen Dalal e Carl Sunshine (1974), que significaram como "*inter"* (entre) e "*network"* (rede eletrônica), este termo passou a designar o ambiente relativo a uma rede de computadores, interconectados.

Conceitualmente considerada um instrumento informático capaz de promover interação entre pessoas de modo virtual[6], permuta de informações e dados, capazes de conectar dispositivos de modo simultâneo através da interligação de equipamentos computacionais, *"máquinas inteligentes*" em rede (CERF; DALAL e SUNSHINE, 1974).

A conexão da internet, por sua vez, se dá a partir de qualquer espaço geográfico que tenha a mesma tecnologia, atuando através de um navegador de suporte mundial conhecido como *world wide web* (www), por sua vez, contém uma infinidade de páginas, textos, imagens e sons, a serem acessadas pelo usuário, quando previamente descodificado. (BERNERS-LEE, 2000)

Ao desenvolver o navegador web foi necessário destrinchar esta tarefa na criação de três tecnologias para que a rede mundial de computadores pudesse efetivamente ter um alcance global, logo, Berners-Lee é considerado o pai do sistema *web* em razão do desenvolvimento desses recursos informáticos possibilitando a navegação global.

Nessa direção, foram criados por Berners-Lee (2000) as tecnologias do *Hypertext Markup Language (*HTML), que permite "*a linguagem usada para criar e escrever documentos ou páginas da web*"; do *Uniform Resource Locato*r (URL), que permite um sistema de localização ou endereçamentos para os documentos produzidos neste ambiente de internet; e

[6] Virtual – ambiente ou local "*fisicamente inexistente, e sim criado por programas de computação, para parecer real aos sentidos (diz-se de imagem ou ambiente)".* Dicionário Houaiss acesso em 25/04/2022. V. (LÉVY, 1996);

do *Hypertext Transfer Protocol* **(**HTTP), protocolo ou idioma que permite comunicação com o navegador e o servidor da internet, visando transmitir documentos através da rede de computadores.

Juntamente com o TCP/IP (*Transmission Control Program/Internet Protocol*), termo inventado por Kahn e Cerf (1974) sistema que permite a transmissão de informações controladas por protocolos e criados para especificar tecnicamente os protocolos da internet, na medida em que encaminha os pacotes de dados por meio da interconexão do navegador com a internet. Tais sistemas unificados permitiram o avanço tecnológico que existe hoje com a difusão e o compartilhamento de dados na rede global, a partir do ambiente cibernético.

Este ambiente cibernético ou ciberespaço[7] é o local etéreo considerado como um local virtual e não físico segundo Johson e Post (1996); é um ambiente acessado através da internet, e por meio do navegador, são realizadas a transmissão e recebimento de dados trocados entre máquinas com capacidade eletrônica computacional, formando uma estrutura digital e eletrônica comunicativa.

Tal capacidade digital concebe uma rede de comunicação atemporal e com alcance global, interconectando todo o mundo, visto não se limita por fronteiras formais físicas como nas interações comuns tradicionais, fato que dinamiza sua utilização e amplia o acesso de troca de informações.

A ampliação do público conectado em quantidade de população, vezes de interação no ambiente cibernético e a ampliação dos recursos tecnológicos, ocasionou inevitavelmente, riscos ligados à engenharia social[8], seja por falta de conhecimento, favorecendo a manipulação e o engano em face dos usuários. (MITNICK, 2002)

Tal realidade levou a criação de tendências preocupantes, atreladas ao consumo das pessoas no âmbito das tecnologias, também, a produção acelerada e artificial de necessidades novas de interação social, incorporando novos modos de vida e a produção de carências e faltas, criando um círculo vicioso de escassez e satisfação, a partir das expectativas, que estimula o uso do digital, como recurso de satisfação pessoal recorrente.

---

[7] Ciberespaço ou espaço cibernético segundo David Johson e David G. Post (1996), é o "lugar" não físico e incorpóreo, descentralizado e distinto da realidade no qual o indivíduo ao utilizar uma senha de acesso, está consciente que está ultrapassando a fronteira da vida real para a vida virtual. "*Law and Borders - the Rise of Law in Cyberspace"* (Lei e fronteiras: a ascensão da lei no ciberespaço);

[8] Engenharia social - são técnicas utilizadas para cooptar acesso a informações sigilosas de usuários ou organizações por meio da internet, a partir das vulnerabilidades ocasionadas pelo próprio utilizador, deste modo, explora a inaptidão, negligência, enganação e manipulação das pessoas no uso desta ferramenta tecnológica. (MITNICK, 2003)

Nesta conjuntura disruptiva tecnológica, as relações dos espaços tradicionais da sociedade, transferiu-se em boa para o ambiente da internet, com vantagens e prejuízos a serem considerados ao longo deste trabalho.

1.2 CIBERNÉTICA E A REVOLUÇÃO TECNOLÓGICA OU INDUSTRIAL “4.0”

Em 1948, o estudioso Norbert Wiener utilizou o termo *Cibernética* para designar o conjunto de institutos sobre teorias de controle e comunicação em uma máquina ou em um animal, seus estudos permitiram ampliar os conceitos e estratégias para facilitar a informação sob a perspectiva de uma medida quantitativa, como é feito com a energia e a matéria, como retrata, Leite da Silva (2014).

Nessa contribuição, permitiu o desenvolvimento intelectual em torno da comunicação e do funcionamento dos computadores, sistemas de controle, comandos eletromagnéticos, transmissões eletrônicas impulsionadas por semicondutores, que possibilitaram produtos autômatos e modernos atuais, contribuindo de sobremodo para o início das tecnologias de automação.

Nessa concepção, Leite da Silva (2014, p.3) informa que a cibernética considerou o “*uso de sistemas de comunicação e consequentemente de seus componentes, que são vitais para troca de informações entre esses componentes, dentro de um mesmo sistema, e também entre o sistema e o ambiente”.*

Deste modo, as tecnologias da atualidade evoluíram dos estudos da cibernética surgidos durante a segunda guerra mundial e tiveram por base, a união das pesquisas sobre a comunicação e a eletrônica, apresentando na primeira fase a busca pela melhoria da comunicação e na segunda fase, evoluir as máquinas informacionais para desenvolver tarefas humanas. (OLIVEIRA, 2009).

Inicialmente a cibernética se desenvolvera em grande parte diante da necessidade de interceptação pelos Estados Unidos da América, da comunicação realizada pelos alemães durante a segunda guerra mundial, posto que através de códigos, informavam a seus prepostos sobre os deslocamento das tropas que deveriam realizar enquanto estratégia de guerra.

Como segunda fase, segundo Oliveira (2009) a cibernética e os avanços tecnológicos que se sucederam levou a temática a tornar-se objeto de estudo das ciências da computação e, passou a ter novo objetivo que se fundamentou na ampliação da capacidade de processamento das máquinas computacionais, em especial, da possibilidade das tecnologias

serem empregadas para o aprendizado das máquinas (*machine learning*)[9], visando à realização de tarefas complexas similares às realizadas pelos seres humanos.

Na contemporaneamente, houve um salto evolutivo no desenvolvimento das máquinas desta área da informática, com a criação de programas e aplicativos que utilizam dos recursos das pesquisas cibernéticas para uso do cotidiano das pessoas, surpreendentemente, continuam a busca que tais máquinas realizem tarefas cada vez mais refinadas e com maior autonomia robótica, inclusive, transformando a perspectiva decisória da máquina, em relação ao ser humano.

Fato é que tais recursos tecnológicos ou máquinas inteligentes permitiram uma infinidade de tarefas a partir da rede mundial de computadores, quando do acesso livre, torna-se instrumento de compartilhamento e também vulnerabilidades, contudo, com inúmeros recursos de interação, sem as limitações existentes nas relações físicas comuns, logo, uma interrelação puramente digital.

Para Oliveira (2009), é importante ressaltar que algumas das máquinas, a partir do aprendizado, já foram capazes de realizar a contento, ações que antes eram exclusivas do ser humano, portanto, tal superação tecnológica já é uma realidade ao superar a capacidade humana em certas tarefas.

Evidencia-se nessa perspectiva, que os recursos computacionais a partir das máquinas aprendentes permanecem em franco processo evolutivo, demonstrando novas vertentes a cada dia, de modo acelerado e até contundente, formando novas concepções sociais e também intervindo na formação do direito.

Nesse sentido, há dois aspectos importantes que não podem deixar de ser analisados, ainda que superficialmente, no processo evolutivo dessa digitalização da vida que são os processos de "*smartificação da sociedade*" e a *"disrupção tecnológica"*, estruturas que potencializam a cibernética e digitalização do mundo.

Nesse sentido, consiste a *smartificação* da sociedade na concepção de XAVIER (2020), no processo de emprego de técnicas de manipulação de grandes dados unidos ao emprego da inteligência artificial e mediante algorítimos que possibilitam uma experiência diferenciada ao usuário, que através de aparelhos telefônicos "*smartphones*" a realização de tarefas complexas levando o individuo a resolver problemas através do aparelho celular.

[9]As máquinas aprendentes *(Machine learning)* evoluíram tecnologicamente, passando a constituir método analítico de dados que a máquina realiza com vistas ao aprendizado das informações e formas de decisões, com a intervenção mínima ou nenhuma do ser humano.

Na mesma direção, as *tecnologias disruptivas* implementadas por essa revolução tecnológica, materializam-se através de equipamentos como televisores, aparelhos celulares, fechaduras digitais, sistemas de iluminação e controle de temperatura, *gadjets* inteligentes e sintetizadores de comunicação como *Siri* ou *Alexa*, estando presente mesmo, em uma singela *panela de arroz i*nterligada a sistemas de internet que permitem automatização do seu emprego em uma cozinha, criando um ambiente digital interligado em rede, com personalização de configurações e tarefas comandadas por voz ou à distância.

Tais características lúdicas e automatizadas ligadas ao investimento na rede tecnológica e na velocidade, criaram nova formatação de um ecossistema de convivência digital, com abordagens personalizadas aos clientes de modo ágil e contínuo, dispostos a criar engajamento consumista quanto aos produtos digitais (HARVARD, 2021); elevando de sobremodo o uso do ciberespaço como local de convivência e resolução da vida.

1.3 SUPERCONECTIVIDADE PANDÊMICA E A VULNERABILIDADE DIGITAL

A superconectividade digital da população aumentou de modo significativo neste estágio informacional, a partir do desenvolvimento da cibernética e da cibercultura[10], então denominada também como era da informação, ou ainda, da indústria 4.0, que tem apresentado pontos positivos e negativos para a convivência humana comunitária, em especial, durante a pandemia que esta geração vivencia exatamente neste momento histórico.

Tal crescimento na utilização do ambiente cibernético, além da evolução comum que já sofria naturalmente pela expansão das novas tecnologias informacionais, passou a ter o reflexo e impacto do fenômeno da Pandemia, que se tornou importante divisor temporal para o aumento da vulnerabilidade digital de boa parte da população, posto que o estímulo e necessidade do uso contínuo do ambiente digital levou a exposição dos seus dados pessoais, vulnerabilizando-os e, por consequência, mitigando direitos fundamentais relevantes.

Há aqui uma racionalização dupla sobre a superconectividade pandêmica exposta nesta pesquisa para melhor compreensão do leitor; de um lado retrata a superconectividade ocasionada pelo aumento do uso da internet durante o momento de pandemia que o mundo presencia neste momento e, de outro, pela compreensão de que há de fato uma

[10] Cibercultura é uma complexidade no imaginário tecnológico que denota uma fantasia relativa à possibilidade de comunicação entre o ser humano e a máquina de modo total; tal vontade se pauta na vontade de estabelecer uma comunicação sem limites, interrelacionando comunidades virtuais para total integração de seres no ciberespaço incorpóreo e flexível. (FELINTO, 2006. p.9)

superconectividade em termos de acesso e adesão de pessoas no ambiente digital em todo o mundo, enquanto uma superconectividade global, em diversos continentes e espaços geográficos, trazendo uma compreensão dupla, porém, interligada destes fenômenos.

O foco do direito nesta conjuntura é revelar caminhos que possam suplantar a preocupação sobre a vulnerabilização do princípio da dignidade da pessoa humana e do seu papel social, na análise do uso maciço e, por vezes, irresponsável ou criminal dos diversos agentes que captam dados neste ambiente digital; notadamente, fragilizando direitos fundamentais a partir da expansão tecnológica que se apresenta.

De modo específico, o período de pandêmica se apresentou com nova dinâmica social por ter sido ocasionada pelo vírus mortal denominado de coronavírus (Sars Covid-19) que levou à necessidade de distanciamento físico entre as pessoas, tendo instaurado no mundo, uma nova forma das pessoas se relacionarem através das redes sociais contidas nas plataformas digitais diversas.

Em 8 de dezembro de 2019, ocorreram os primeiros registros do coronavírus em um hospital da cidade de *Wuhan* na China e em janeiro de 2020, representante da Organização Mundial da Saúde (OMS) informou sobre a potencialidade da doença transformar-se em uma pandemia se alastrando pelo mundo, o que viria a ser um prelúdio de uma devastação sanitária mundial.

Diversos países passaram realizar imediata prevenção sanitária, tendo o Brasil expedido Decreto Federal de *emergência sanitária* em 6 de fevereiro de 2020, e tendo registrado o primeiro caso confirmado de coronavírus no dia 26, no Estado de São Paulo.

Desde esse Decreto nº 13.979, de 6 de fevereiro de 2020[11] do Governo Federal que dispôs "*sobre as medidas para enfrentamento da emergência de saúde pública de importância internacional decorrente do coronavírus responsável pelo surto de 2019"* e a Emenda Constitucional 106/2020 que instituiu o denominado *orçamento de guerra* que facilitou os gastos no combate à pandemia através do orçamento da União, o distanciamento social foi um dos principais instrumentos de prevenção.

Em razão da inexistência de conhecimento suficiente sobre a doença e a carência de vacinas e recomendação da OMS diversos países e, entre eles, o Brasil, houve a necessidade de fechar todo o comércio, a indústria e os ambientes de interação pública, promovendo um

[11] O fim da Emergência em Saúde Pública de Importância Nacional (Espin) foi anunciado pelo Ministro da Saúde em 17 de abril de 2022, tendo a Casa Civil neste período registrado mais de *"660 atos normativos relacionados à covid-19",* entre eles, 94 leis e decretos, portarias e resoluções diversas. (SENADO, 2022)

distanciamento físico generalizado, que teve como consequência principal, a busca da população pelo uso da rede de internet para a interação social.

O contexto de distanciamento social deste período ocorrera formalmente a partir de medidas governamentais que levaram ao fechamento do comércio, instituições, escola e a diversidade de negócios comuns, no qual o meio cibernético tornou-se a principal fonte de informação e meio de relação entre as pessoas, inclusive, da realização de tarefas de trabalho, entretenimento, entre outras; fato que acelerou o uso das ferramentas digitais no Brasil e no mundo, de modo simultâneo e em larga escala, aumentado o acesso ao ambiente digital.

Fato é que toda essa dinâmica criou um novo fenômeno na população pela impossibilidade da presença física tradicional nas relações, exceto na prestação dos serviços essenciais, tendo por consequência a superconectividade das pessoas para resolução dos problemas através de meios digitais, estabelecendo novos parâmetros de relacionamento social, econômico, cultural e de trabalho, a partir do teletrabalho ou *"home office".*

As restrições ocasionadas pela pandemia levaram ao distanciamento físico de cunho comunitário, de modo mais radical entre março/2020 a dezembro/2021, porém, mesmo com certa relativização do distanciamento após esse período com o advento da vacinação em massa da população, o país ainda conta os seus mortos em mais de dois anos de pandemia.

Alguns dos impactos diretos do fenômeno da pandemia foram à utilização dos recursos do ciberespaço para a realização de atividades digitais em um patamar jamais visto historicamente. Essa peculiaridade sanitária contribuiu para acelerar de modo significativo o processo de digitalização de diversas nações, das suas organizações públicas e privadas, das empresas e pessoas, a partir da necessidade de sobrevivência econômica e social.

Segundo o Centro de Ciência e Engenharia de Sistemas da *Universidade de Johns* Hopkins (2022)[12], o total de casos diagnosticados no mundo ultrapassaram 634 milhões de pessoas infectadas pelo sars covid-19, das quais mais de 6,6 milhões de pessoas foram a óbito.

O Brasil, por sua vez, registrou 34,9 milhões de infectados e mais de 688,6 mil de óbitos, com uma população de 112 milhões de habitantes[13], entretanto, as nações mais desenvolvidas construíram estruturas de acesso à internet e atuação digital significativa.

[12] V. dados em tempo real da Universidade Johns Hopkins. Disponível em https://coronavirus.jhu.edu/map.html Acesso em 13 Dez. 2022.
[13] Estimativa da população segundo o Instituto Brasileiro de Geografia e Estatísticas- IBGE em 23 Nov. 2022;

Atualmente, o movimento tem sido de retorno às atividades presenciais em razão da população mundial estar sendo imunizada, cuja aplicação de vacinas já superou 12,8 bilhões de doses, segundo aquela Universidade. (JOHNS HOPKINS, 2022)

Não obstante, há que ressaltar que essa não é uma realidade no plano global, em razão da vacina ser fruto de investimentos em pesquisas tecnológicas e muitos países pobres do continente africano possuem enorme carência nesta produção científica, assim sofreram com duas dinâmicas distintas ligadas ao empobrecimento histórico que possuem.

Países da África apresentaram falta de estrutura digitalizada para a população acessar serviços públicos assistencialistas de modo digital, fato que diante do distanciamento físico, comprometeu relações econômicas significativas, com impacto no aumento da fome.

Para fins de comparação com a realidade pátria, apesar das enormes dificuldades quanto à inclusão digital[14], especialmente no tocante à população pobre, o Brasil forneceu assistência emergencial pecuniária através do sistema bancário digital a mais de 67 milhões de pessoas que não estavam no sistema bancário, durante a pandemia. (PINTO, 2020).

No segundo aspecto de análise, foi observado em países africanos, que há enorme escassez e lentidão no acesso às vacinas para a imunização da população, mesmo após quase dois anos de início desta imunização no mundo, diferentemente do que ocorre na maioria dos países desenvolvidos, ou mesmo, em desenvolvimento como o Brasil.

A título de exemplo, enquanto países ricos apresentam alto índices de pessoas vacinadas com a primeira dose, como ocorre na China que está com 92,6% da população imunizada, Japão com 82,6%, na Europa, Portugal alcançou 95,8% de pessoas vacinadas, Espanha com 88,4%, Itália com 84,1%, França com 83,7%, apresentando também, bons índices na América Latina, com a Argentina tendo 91,6% da população imunizada, México com 72,5%, Chile com 94,6% e o Brasil possuindo 88,5% da população vacinada.

Na contramão, África sofre com o baixo investimento em tecnologia sendo dependente da produção de ciência de outros continentes, como pode ser visto pela cobertura vacinal de *Camarões* que apresenta apenas 11,1% de pessoas imunizadas contra a Covid-19, *Senegal* com 11,6% de vacinados, *Mali* com 14,5%, *Gabão* 14%, *Sudão* 22,6% e *Namíbia* com 23,6% de imunizados. (JOHN HOPKINS, 2022)[15]

[14] Tramita no Brasil a PEC 47/2021, que estabelece a inclusão digital no rol dos direitos e garantias fundamentais do país, de modo a reduzir as desigualdades na população que não tem acesso ao ambiente digital. V. https://www.congressonacional.leg.br/materias/materias-bicamerais/-/ver/pec-47-2021;

[15] Consulta em 13 Dez. 2022. (HOPKINS, 2022). Disponível em https://coronavirus.jhu.edu/map.html.

Evidenciando que a falta de produção cientifica e tecnológica no âmbito da saúde, além da distribuição desigual, ampliam as desigualdades sociais e interferem na assistência direta a vida, dada a carência de investimentos na proteção sanitária e saúde pública nessas nações.

Em outra vertente, a pandemia também influenciou no valor sobre os dados no ambiente digital, fato surpreendente foi a *ressignificação dos dados* das pessoas e das empresas como objeto de valor negocial, uma espécie de *ouro digital* ou *petróleo do século XXI*, que elevou o valor econômico e político dos dados cooptados no meio digital, alçando tais informações ao estatus de objeto de interesse e valor econômico para manipulações diversas, por vezes, favorecendo inclusive a estrutura de organizações criminosas sofisticadas.

Nessa direção, a superconectividade da população em rede também, favoreceu a atuação da criminalidade que transmutou seu ambiente de atuação para o espaço cibernético, logo, tal modificação social, não passou despercebida aos olhos dos cibercriminosos que passaram a cometer crimes em massa, deixando de lado o método tradicional ou ainda, mesclando a modalidade com o meio digital.

Nessa transformação comportamental, tal fenômeno também não seria ignorado pelas grandes Corporações do ramo da tecnologia *Big Techs* e consumerista, que viram nos dados dos usuários uma fonte de poder econômico (entre outros), favorável às finalidades corporativas e econômicas, além de políticas.

Ademais, convém considerar que as máquinas, *hardwares e softwares,* atualmente já são capazes de manipular grande número de informações com a tecnologia do "*big data*" e através da inteligência artificial, já realizam tarefas de alta complexidade, aproximadas às dos seres humanos, capazes de manipular processos decisórios dos usuários que atuam nas redes sociais ou se utilizam dos imensuráveis serviços da internet.

Defende-se, portanto, a necessidade de conhecer os riscos que as principais tecnologias da inteligência artificial apresentam e como podem impactar na dignidade da pessoa humana, posto que a união dos fenômenos da superconectividade acelerada e a revolução ocasionada pela forma das máquinas informáticas atuarem na contemporaneidade, capazes de realizar tarefas com alta complexidade, abriram um caminho fértil para a vulnerabilização de bens relevantes.

Nesta direção, é preciso considerar que os princípios e direitos constitucionais inerentes aos dados, devem ser tutelados pelo direito para que não sejam objetos de desfacelamento sob qualquer pretexto.

2. NEOCONSTITUCIONALISMO E A INTERPRETAÇÃO *"PRIMA FACIE"* DO PRINCÍPIO DA DIGNIDADE DA PESSOA HUMANA

A proteção das relações sociais sob o princípio da dignidade da pessoa humana é imprescindível para manutenção da igualdade e da vida em sociedade, ainda que confrontados com os avanços tecnológicos deste início de século.

Os melhores recursos da tecnologia desta era informacional ainda que determinem benefícios diversos e proponham um novo modelo de vida coletiva, não podem apresentar retrocessos na construção histórica dos direitos humanos, nem podem permitir a relativização dos direitos fundamentais que foram consolidados como pressupostos da vida comunitária.

É preciso desenvolver a compreensão de que as normas constitucionais deste novo século, devem ser lidas pela sociedade para além do seu contexto formal e funcionalista positivado, a regra constitucional precisa ser regida por uma eficácia equitativa que considere no caso concreto o alcance da justiça, posto que não objetiva a produção de injustiças, ao contrário. (FERRAZ JR, 1989)

Apesar da norma constitucional apresentar uma clara função positivada, a correspondência entre justiça e direito nem sempre esteve presente no resultado social, portanto, há a necessidade de inovação no método hermenêutico na qual se assenta a interpretação da norma constitucional, que vá além do aspecto da legalidade formal, posto que por vezes, permitiu o exercício do direito injusto.

É necessário buscar a legitimidade social da norma constitucional, através da satisfação política da sociedade, ou seja, de ordem axiológica, cuja interpretação deve estar voltada a realização de valores da coletividade, sob a perspectiva de justiça social (FERRAZ JÚNIOR, 1990); possivelmente de modo aproximado ao que Ricardo Maurício Soares (2008) denomina de *Direito Justo*.

Nesse contexto, há uma necessidade de superação da estrutura interpretativa das leis constitucionais do século XIX e do início do século XX que direcionavam a interpretação à estrita legalidade formal, à lei positivada, sem analisar a perspectiva valorativa e o que de fato se desejava alcançar com a norma.

Este método interpretativo do século XIX, já não atende mais aos desejos deste início de século XXI e seus desafios, posto que revelou limitações e incoerências, no

atendimento às aspirações sociais que reclamam a efetiva realização política da norma, enaltecendo o viés valorativo que a atual interpretação impõe. (FERRAZ JR, 1989)

Como retrata o professor Edvaldo Brito (1993, p.117) o texto constitucional possui três conteúdos relevantes que devem ser considerados: o semântico, sintático e pragmático, formando a estrutura da constituição; do ponto de vista semântico, revela signos formais exigidos pela técnica e que possuem o objetivo de restringir significados e convencionar a linguagem adequada.

Na perspectiva sintática surgem vinculações que levam o interprete a se vincular ao texto constitucional e, na perspectiva pragmática, existe a interpretação da norma deve ser compreendida à luz das aspirações sociais, enquanto um pacto jurídico (BRITO, 1993), cuja norma constitucional deve ter consonância com o corpo social em sua máxima expressão.

Nesse sentido, os princípios constitucionais sinalizados ou positivados enquanto norma-princípio tem legitimidade no entendimento do texto, somente se utilizados de modo entrelaçado. O Estado instituído como Democrático de Direito absorve o direito humano inalienável contido nas normas desta carga magna, tendo como raiz fundamental as vontades da sociedade civil, ao passo em que são guardados por uma jurisdição especial e específica, a do juiz natural, que dá efetividade ao instituto. (BRITO, 1993)

É exatamente no contexto deste direito constitucional pragmático que o neoconstitucionalismo vem traçando suas bases teóricas. Como reforça Dirley da Cunha Júnior (2021, p.41), o surgimento dessa teoria constitucional surgiu do movimento ocorrido após a 2ª guerra mundial e visou consolidar o Estado constitucional de direito centrado nos direitos fundamentais com uma compreensão diferente do constitucionalismo positivista que lhe antecedeu, na qual as pretensões jurídicas eram limitadas à norma expressa.

Este neoconstitucionalismo tem o condão de estabelecer um novo paradigma sobre os direitos fundamentais e a concepção de um Estado constitucional de direito, aproximando os direitos fundamentais da ética, da moral e do sentido de justiça e outros valores substantivos. (CUNHA JÚNIOR, 2021, p.43)

Permite-se então, uma nova forma de conceber a interpretação a partir do viés axiológico, intimamente relacionado à proteção da dignidade da pessoa humana e dos direitos fundamentais, tais institutos, por sua vez, devem ser resguardados mesmo diante da evolução tecnológica que se apresenta, assim, cobrando das tecnologias que estas precisam se amoldar à proteção social. Na concepção de Dirley da Cunha Júnior, sobre a importância dos princípios jurídicos e a relevância da valoração constitucional, este resume que:

> os princípios jurídicos, sejam explícitos ou implícitos, são normas jurídicas dotadas de normatividade, que, por via de consequência, obrigam e vinculam, distinguindo-se das regras na medida em que eles são normas providas de intensa carga axiológica (referem-se diretamente a valores), enquanto as regras jurídicas são normas descritivas de situações fáticas hipotéticas, dispostas a *concretizar* os valores normatizados pelos princípios. (CUNHA JÚNIOR, 2021. p.153)

No exercício do neoconstitucionalismo, o texto constitucional pode ir além do expresso na carta magna, englobando e aplicando o direito para a verdadeira justiça ou mesmo o direito justo de modo a promover o reconhecimento dos princípios e se amoldar à interpretação do direito para alcançar o objetivo dogmático constitucional relacionado aos valores que deseja proteger, promovendo uma expansão jurídica constitucional que permite solucionar antinomias, com base na ponderação. (CUNHA JÚNIOR, 2021)

Na concepção de Robert Alexy (2008, p.450 e 453) o direito a proteção deve estar disponível ao titular em face do Estado ou em face de terceiros, posto que pode haver intervenção de terceiros, podendo também apresentar o Estado como violador, quando não cumpre de modo suficiente o seu dever de proteção, comprometendo princípios fundamentais.

Diante da necessidade de tal proteção, o que se analisa é que os riscos inerentes às tecnologias computacionais e o uso da inteligência artificial, inauguram uma discussão sobre a proteção de institutos de direitos fundamentais relevantes da sociedade, como o recém-constitucionalizado direito à proteção de dados e o direito à privacidade e o impacto no princípio da dignidade da pessoa humana, constitucionalmente estabelecido. (CRFB, 1988)

Para Alexy (2008, 91; 103), na teoria dos direitos fundamentais os princípios são mandamentos de otimização *prima-facie* que visam o alcance e realização efetiva do direito, ou seja, mandamentos que devem ser interpretados adaptando seu sentido para atender as vontades sociais. Tal modelo interpretativo vincula o sistema jurídico positivado (escrito) a um sistema ético e moral, de modo a alcançar o objetivo maior axiológico (valorativo) da norma. Nesse sentido, os princípios emitem ordens ao intérprete, que devem ser obedecidos a partir da adaptação do direito aos objetivos do direito. (ALEXY, 2008).

Na análise das tecnologias de ultima geração, seguindo tal raciocínio, estas precisam estar condizentes com o princípio da dignidade da pessoa humana para que não desgarrem do seu objetivo maior de satisfação da política social, mesmo diante das benesses e criatividades que as evoluções tecnológicas possam apresentar, portanto, a evolução tecnológica sempre estar adstrita ao caráter *prima facie* dos princípios e direitos fundamentais.

2.1 COMPREENDENDO O PRINCÍPIO DA DIGNIDADE DA PESSOA HUMANA

Para que tal compreensão possa ser mais bem delineada, faz-se necessário se debruçar sobre as noções da dignidade humana diante da perspectiva histórica e como este instituto se constituiu como direito, posteriormente se convertendo no marcador principiológico que conhecemos na contemporaneidade.

A dignidade humana na pretensão de *Immanuel Kant*[16] tem por pilar a autonomia da pessoa humana como imperativo de conduta, e em sua função singular que não pode ser precificada com valor econômico restando-lhe a dignidade, em razão da capacidade de estar acima de qualquer precificação, o que lhe encerra um caráter único. (Kant, 2004 apud Barroso, 2010; p.18)

Nessa direção, há o imperativo categórico de que "*todo ser racional existe como um fim em si mesmo, e não como meio para o uso arbitrário pela vontade alheia"* (Kant, 2004 apud Barroso, 2010; p.16); cujas vontades e condutas humanas estão interligadas às condições humanas natas, intimamente relacionada à afetividade e a solidariedade, mas também, que se interligam aos arroubos da vontade de riqueza e de poder, revelando a necessidade do indivíduo viver dentro de uma moral que lhe permita superar seus instintos e interesses. (Barroso, 2010)

Deste modo, mesmo antes do levante, diversas normativas internacionais de direito e constituições de diversos países o princípio da dignidade da pessoa humana já figurava como um objeto de valor axiológico, ligado à cultura humana, construído inicialmente como um ideal metafísico, dentro uma concepção histórico-cultural, surgida como um sistema de valores humanos. (SOARES, 2008, p.160)

Na contemporaneidade a dignidade humana tornou-se refinada e se compactou em uma proposição ímpar, tornando-se representativa de uma inspiração para a conduta ética, tornando-se um ícone universal a ser buscado.

As pessoas, nessa direção, devem continuar mantendo sua característica de ser humano não como objeto ou função de vontades externas, ou alheias, posto que *"não têm preço nem podem ser substituídas, possuindo um valor absoluto, ao qual se dá o nome de dignidade"* (BARROSO, 2010, p.19); notadamente, com um supravalor impossível de quantificar.

[16]Immanuel Kant é considerado o maior expoente da filosofia europeia moderna, tendo discutido sobre autonomia e dignidade como fruto do período Iluminista e da Revolução Francesa, nos quais os direitos fundamentais passaram a ser discutidos como pilares do sistema de normas. V. (KANT, 2004);

Nessa linha, reporta-se Soares (2008, p.177), que o conceito de dignidade da pessoa humana "*não será propriamente lógico-jurídico, porquanto não se pode defini-la em termos universais e absolutos. A delimitação do significado ético-jurídico de que o ser humano é um fim em si mesmo deve ser buscada em cada contexto histórico-cultural".*

Assim, a dignidade não deve ser pensada apenas como algo relacionado à natureza do homem, mas como elemento cultural, fruto das conquistas geracionais que impactam no direito e exercício de direitos devendo ser reforçado ao longo do tempo.

Note-se, que apesar de ter se tornado uma lei universal a dignidade deve ser pensada enquanto um conceito amplo, plástico e plural, mas que passou historicamente a representar um ideal simbólico do valor da pessoa humana e, como consenso, inerente aos fundamentos dos direitos humanos. (BARROSO, 2010)

Tanto, que é invocada em diversas áreas do conhecimento humano "*da bioética à proteção do meio ambiente, passando pela liberdade sexual, de trabalho e de expressão"*, além de representar-se de modo transnacional, fato que envolve situações históricas, religiosas e políticas de nações diversas, o que impossibilita uma reflexão unificada e exige neutralidade para que permaneça com a característica da universalidade. (BARROSO, 2010; p.19/20)

Para melhor explicitar, retrata o nobre Ministro Luís Roberto Barroso:

> Em verdade, dignidade humana e direitos humanos são duas faces de uma só moeda, ou, na imagem corrente, as duas faces de Jano[17]: uma, voltada para a filosofia, expressa os valores morais que singularizam todas as pessoas, tornando-as merecedoras de igual respeito e consideração; a outra, voltada para o Direito, traduz posições jurídicas titularizadas pelos indivíduos, tuteladas por normas coercitivas e pela atuação judicial. Em suma: a moral sob a forma de Direito (BARROSO, 2010; p.21)

Do ponto de vista normativo que contribuiu para essa convergência legal da dignidade humana para o arcabouço do direito, o grande avanço ocorreu justamente a partir das desumanidades, tortura e do genocídio étnico cometido contra diversos seres humanos durante o período de guerra finalizado em 1945.

---

[17] *Jano* é um *Deus* romano ligado às mudanças, transições, escolhas e decisões (portas de entrada e saída); possuía duas faces, uma voltada para a frente e a outra para trás refletindo o passado e o futuro; ele foi grande inventor e o primeiro a cunhar moedas de bronze, o que levou países como Grécia e Itália a terem moedas quer representam as suas duas faces, ou ainda, quatro faces representando as diversas fases de maturidade do homem. (FERNANDES, 2021)

Os regimes totalitários dominantes à época, além do histórico de crueldade envolvendo processos de escravidão e extermínio de seres retratados em outros estágios da história, o reconhecimento do homem enquanto detentor de direitos políticos da República, contribuiu para que o princípio da dignidade da pessoa humana, fosse considerado enquanto um limite na perspectiva do direito. (SOARES, 2008, p.164/6)

A dignidade da pessoa humana passou a se configurar como fonte dos direitos fundamentais, translocando o fenômeno jurídico protetivo para o respeito à condição do ser humano "*como valor supremo dos sistemas jurídicos de inspiração democrática"* como retrata Ricardo Maurício Soares (2008, p.164).

O grande marcador histórico para tal convergência foi à criação da Organização das Nações Unidas (ONU) em 24 de outubro de 1945, e a Declaração Universal dos Direitos Humanos (DUDH) em 10 de dezembro de 1948, inaugurando um levante no emprego da dignidade humana como pressuposto a ser considerado em qualquer circunstância social, instituindo-o formalmente no âmbito do direito.

A partir das normas aprovadas pela Assembleia Geral das Nações Unidas, cujos 48 países-membros votaram a favor e nenhum contra, a dignidade humana tornou-se o *mínimo ético fundamenta*l a ser assegurado de modo universal, posto que tais normas eram *"indiscutivelmente vinculantes do ponto de vista jurídico"*. (BARROSO, 2010; p.21)

Tal representatividade da dignidade humana no plano jurídico permitiu que o valor intrínseco da pessoa humana fosse elevado a uma grande importância e impôs a inviolabilidade desta dignidade no plano social, resultando em uma cascata de direitos fundamentais (BARROSO, 2010); considerados parcelas do exercício dessa dignidade.

Resultam deste valor, intrínseco à pessoa humana, segundo Barroso (2010) sob o lastro do ordenamento jurídico: o direito à vida, à igualdade, à diversidade, à integridade física, incluindo, a proibição da tortura, do trabalho escravo e penas cruéis.

Na mesma direção, a proteção da integridade moral ou psíquica contra a violência simbólica, além de abranger o direito à privacidade, enquanto um conjunto ligado à intimidade, à honra e à imagem (BARROSO, 2010), bem como, o reconhecimento da proteção dos dados pessoais no plano atualizado.

É possível identificar o aspecto da integridade física e moral que é atributo inerente a todos os seres humanos do mundo, mas referem-se, também, a perspectiva espiritual, às condições materiais de sobrevivência do indivíduo, visando protegê-lo da coisificação e da degradação em sociedade. (SOARES, 2008, p.177)

Fato é que a normativa internacional levou Estados soberanos e do direito internacional a empregar a dignidade humana como pressuposto de direito justo, como revela Ricardo Maurício Soares tornado-se parâmetro de ordenamento. (SOARES, 2008)

Nessa acepção, o *Direito Justo* passa a estar intimamente ligado à dignidade da pessoa humana em razão do seu fundamento último e da racionalidade em essência que apresenta, sendo compreendido na acepção de Ricardo Maurício Soares como:

> Direito justo não é outro, senão o próprio homem, considerado em sua dignidade substancial de pessoa, como um ser que encerra um fim em si mesmo, cujo valor ético intrínseco impede qualquer forma de degradação, aviltamento ou coisificação da condição humana. (SOARES, 2008, p.157)

No plano nacional, a Constituição da República Federativa do Brasil (CRFB, 1988) permitiu a internalização dos institutos normativos internacionais trazendo à dignidade da pessoa humana para o centro do ordenamento jurídico, dando-lhe caráter de norma fundamental e estruturando tal valor como pilar de todo o sistema constitucional estabelecido.

A carta magna brasileira permitiu deu a dignidade humana perspectiva norteadora no complexo portfólio de direitos fundamentais que traduz, em especial, dos que resguardam direitos relevantes constantes do artigo 5º como a vida, liberdade, segurança, propriedade, igualdade, intimidade e a proteção de dados pessoais, entre outros institutos (SOARES, 2008; p.168); tornando-a princípio.

A dignidade da pessoa humana foi alçada a baluarte principiológico interpretativo das normas ali inseridas, hermeneuticamente defendido nesta pesquisa, enquanto um máximo existencial a se buscar, com base nos objetivos da nação retratados no art. 3º e seus incisos (CRFB, 1988).

Nessa direção, expressa o texto constitucional quanto aos objetivos fundamentais, a necessidade de permitir a construção de "*uma sociedade livre, justa e solidária",* pautada no "*desenvolvimento nacional",* que busque *"erradicar a pobreza e a marginalização*", reduzindo desigualdades e promovendo o "*bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação*". (BRASIL, 1988; art.3º)

É necessário alertar, entretanto, que o catálogo disposto na constituição é uma relação aberta e inconclusa que expressa garantias fundamentais e direitos, que não excluem outros direitos decorrentes de outros regimes oriundos da internacionalização das normas, também, não se encerram no artigo quinto, estando espalhado por toda a normativa constitucional. (SOARES, 2008; p.170)

Nessa direção, convém analisar que a perspectiva valorativa da dignidade da pessoa humana no advento da teoria do neoconstitucionalismo atualmente proposto, dá a este instituto uma concepção ainda maior, ampla e viva, posto que cobra uma concretude ligada aos fatos da vida em sociedade, transbordando do texto constitucional a partir de uma interpretação teleológica e axiológica da norma.

Este fundamento do direito passou a convergir sob diversas dimensões do direito, visando tornar-se realidade no plano social como delineia Soares (2008, p.170), se impõe por meio da dimensão da validade (visão normativa), da efetividade (visão fática) e da legitimidade (visão valorativa), dentro do sistema jurídico; com foco na execução de um direito justo como já delineado, sendo representado como um supraprincípio jurídico.

Como retratado por Alexy (2008), no tocante aos princípios constitucionais postos à sociedade, estes devem ser protegidos de terceiros e do próprio Estado, posto que ambos podem se demonstrar violadores. Nesse sentido, a interpretação axiológica deve permitir maximizar tais princípios promovendo através da hermenêutica, um ato discricionário do intérprete correlato a uma efetividade de justiça no plano social; ou seja, que permita o direito justo de modo isonômico a todas as classes sociais.

Nessa concepção, o princípio específico da dignidade da pessoa humana se apresenta como uma determinação máxima capaz de se aplicar ao caso concreto, cobrando eficácia e efetividade a partir da interpretação jurídico-axiológica, que possa convergir em ação e realidade, na lógica do máximo existencial; ademais, superando a aplicabilidade do *mínimo existencial*[18], historicamente defendido por muitos pesquisadores.

Nessa direção, conceituando o princípio da dignidade da pessoa humana, por sua vez, Barroso (2010, p.12-13) retrata que este surge como fundamental e passa a exigir o reconhecimento de toda a hermenêutica constitucional e infra para a sua efetividade; regendo, limitando e condicionando o sentido das normas jurídicas para os seus objetivos e alcance.

Deste modo, no processo decisório de implementação das tecnologias na sociedade não pode destoar de tais objetivos, seja no plano político, econômico ou social, posto que todos os instrumentos sociais precisam se coadunar com o pensamento ético e moral compatível com o princípio da dignidade da pessoa humana expressos, devendo ser operacionalizado a partir da parcela dos direitos fundamentais existentes.

[18] O mínimo existencial ou vital é retratado como a parcela assistencial discricionária do poder público para garantir o sustento e sobrevivência da pessoa, conforme art. 38 da Constituição da Itália, como discute Pizzolato em sua obra *O mínimo Vital*. (2004, p. xii)

Tais concepções, diante do uso das tecnologias informáticas e diante da afetação e vulnerabilização dos dados sensíveis, levam a conclusão de que toda e qualquer tecnologia aplicada em massa no seio social.

É necessário estabelecer um método de frenagem para que princípios relevantes e os direitos fundamentais não sejam dilacerados ou mitigados, a partir de limites bem construídos pelo próprio direito, para proteção da coletividade humana.

Por fim, entende-se que é necessário o pleno reconhecimento da dignidade humana como instituto a ser protegido pelo ordenamento jurídico, inclusive, na esfera da aplicação das tecnologias e avanços da indústria robótica e da inteligência artificial de hoje.

Em razão da necessidade humana de zelar pela igualdade nas condições de acesso a essa dignidade, que como revelou Hannah Arendt deve ter a pluralidade presente na oferta da dignidade como condição humana e política de sobrevivência, mesmo diante dos desafios sociais que se apresentam. (ARENDT, 2002; p.15)

2.2 DIREITO À PRIVACIDADE E À PROTEÇÃO DOS DADOS SENSÍVEIS

Destina-se esta parte a analisar o direito fundamental à privacidade, conforme expresso no artigo 5º, inciso X, e o direito fundamental à proteção dos dados das pessoas, constante do artigo 5º, inciso LXXIX, ambos da Constituição Federal do Brasil (1988).

Note que a proteção de dados das pessoas foi instituto recentemente alçado à categoria constitucional e sua classificação se encontra delineada como dados *sensíveis* na Lei Geral de Proteção de Dados (LGPD, 2018).

Como visto anteriormente, a gênese fundada nas normas internacionais levaram diversos direitos fundamentais a serem nacionalizados, compondo o texto da Constituição Federal pátrio a partir de 1988, fato que permitiu uma concepção amplificada de diversos institutos de direitos humanos, transformando o arcabouço normativo do Brasil.

No tocante ao direito fundamental à privacidade, que encerra um conjunto de direitos fundamentais, a constituição tratou de protegê-la para tutelando especificamente o direito à inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, portanto, consagrando a expressão ‘privacidade’ em sentido amplo, como se apresenta no artigo 5º, inciso X. (CUNHA JÚNIOR, 2021, p.662)

Nesta compreensão, a privacidade abrange a personalidade individual que se manifesta na intimidade e, na qual cada indivíduo pode obstar ou proibir interferência, ou a divulgação de informações; reflete também nessa perspectiva l*ato sensu*, a partir do modelo

interpretativo extensivo, o direito de estar só e também de ser deixado em paz, como também, de tomar decisões autônomas na esfera de sua vida privada, sem interferência de terceiros. (CUNHA JÚNIOR, 2021)

Ainda, segundo Cunha Júnior (2021), o direito à intimidade se refere à vida secreta e reservada do cidadão, estando ligada a essência e personalidade de cada um; a vida privada, menos secreta, refere-se à vida familiar, no trabalho, na relação com amigos das pessoas e, cujas informações podem ter certa reserva.

No âmbito do direito à honra refere-se à consciência sobre dignidade pessoal e sua reputação social além do direito de imagem, que orbita no âmbito da utilização dos atributos físicos do indivíduo para caracterizar ou representar alguma coisa, ou pessoa. (CUNHA JÚNIOR, 2021)

Na direção da prestação estatal do direito fundamental à privacidade, expõe Doneda (2006), que o direito à privacidade teve uma transformação significativa em relação ao período histórico anterior, posto que se consubstanciava em um direito negativo do Estado, ou seja, de não intervir no seu livre exercício.

Entretanto, em razão da extensa vulnerabilidade da intimidade das pessoas, em especial, pelo aspecto midiático que a sociedade alcançou em razão das tecnologias digitais, esta condição foi alterada, tornando-se do direito fundamental à privacidade, um direito positivo a ser promovido pelo Estado, pela necessidade de iniciativa protetiva a partir desta nova natureza prestacional.

Tal posição positiva prestacional diante do direito à privacidade se coloca em posição de destaque para a tutela do princípio da dignidade humana a partir da proteção da intimidade das pessoas. Com retrata nesse sentido Doneda:

> A privacidade assume, portanto, posição de destaque na proteção da pessoa humana, não somente tomada como escudo contra o exterior – na lógica da exclusão – mas como elemento positivo, indutor da cidadania, da própria atividade política em sentido amplo e dos direitos de liberdade de uma forma geral. Neste papel, a vemos como pressuposto de uma sociedade democrática moderna, da qual o dissenso e o anticonformismo são componentes orgânicos (DONEDA, 2006, pp. 141-142).

Por tudo, o direito fundamental à privacidade torna-se objeto e baluarte da prestação positiva do Estado que deve, nessa nova concepção, gerar a liberdade plena do seu usufruto do direito, mas também, agir na produção de ações para restringir o acesso desmedido à intimidade,

honra e imagem das pessoas, contra a violação do próprio Estado e dos particulares, em especial, com o advento das tecnologias digitais avançadas.

No estudo do direito fundamental à proteção de dados das pessoas, por sua vez, expresso no inciso LXXIX do artigo 5º da CRFB (1988), instituto como já citado, recém-constitucionalizado através da Emenda Constitucional nº115 de 2022, este teve sua gênese jurídica no Brasil através da normativa ordinária da Lei Geral de Proteção de Dados (LGPD) nº 13.709 de 14 de agosto de 2018, com alterações na Lei nº 13.853, de 2019.

É importante, deste modo, realizar a leitura do conteúdo constitucional, entrelaçando o olhar com a LGPD (2018), que conceitua, por exemplo, no seu artigo 5º, inciso I, o que é dado pessoal. Deste modo, dado pessoal é a "*informação relacionada à pessoa natural identificada ou identificável*"; na mesma direção, conceitua banco de dados como o "*conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;".*

Enquanto o texto constitucional expresso no inciso LXXIX do artigo 5º (CRFB, 1988) assegura "*o direito à proteção dos dados pessoais*" é relevante constatar que a norma constitucional expõe a proteção dos dados sensíveis que tramitam de modo tradicional entre indivíduos, instituições e órgãos governamentais, quanto aos que tramitam por meio eletrônico como expressa: "*inclusive nos meios digitais".*

Na mesma direção protetiva, a Lei de Dados (2018) que nasceu para dispor sobre o "tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.", trouxe regulamentações que servirão a execução do direito fundamental constitucional maior.

O surgimento desta norma se deu para regular o texto constitucional com vistas a proteger direito dos usuários, diante da devassa dos dados no âmbito digital, relacionando também, tal proteção da privacidade e dos dados pessoais ao princípio da dignidade da pessoa humana, de modo expresso.

Como expõe no art. 2º, a LGPD (2018) disciplina que a proteção de dados está fundada na perspectiva constitucional do: "*respeito à privacidade"* (inciso I); "*a autodeterminação informativa*" (inciso II); "*a liberdade de expressão, de informação, de comunicação e de opinião*" (inciso III); "*a inviolabilidade da intimidade, da honra e da imagem*" (inciso IV); "*o desenvolvimento econômico e tecnológico e a inovação*" (inciso V); "*a livre iniciativa, a livre concorrência e a defesa do consumidor*" (inciso VI); e "*os direitos*

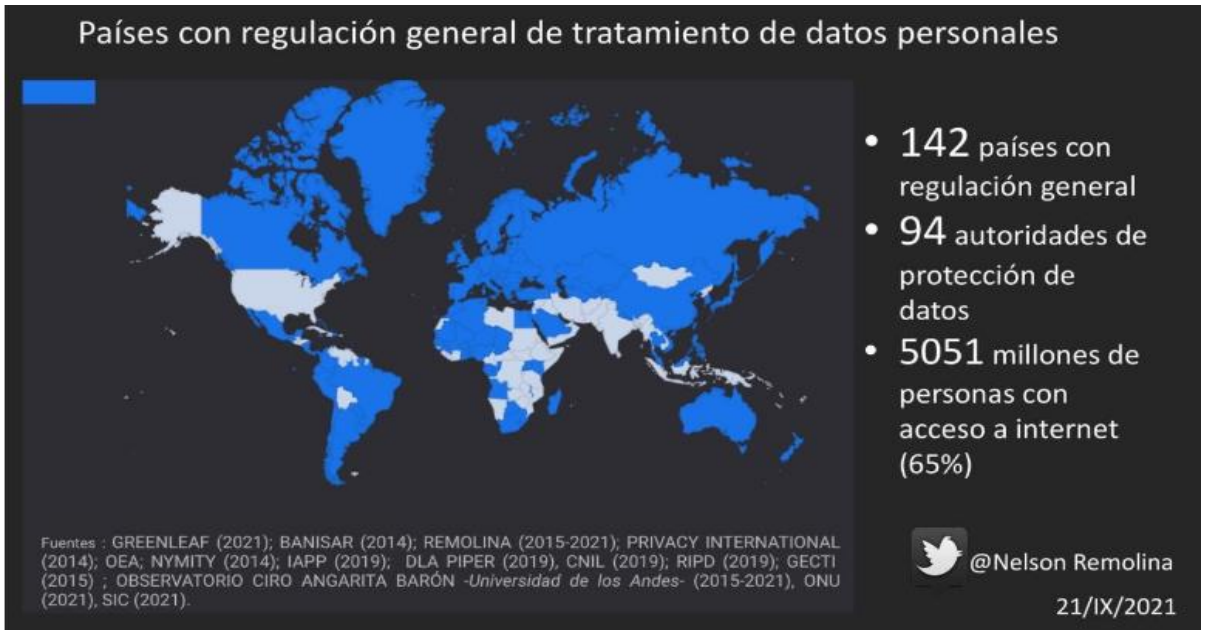
humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais" (inciso VI).

A LGPD (2018) passou a ser direcionada a todos aqueles que, de alguma forma, captam informações sobre indivíduos e instituições, em especial, para fins econômicos, tanto no meio digital ou físico; foram criadas melhorias no âmbito negocial prevenindo a concorrência desleal a partir do regramento sobre dados.

Para a relatora especial da ONU para a privacidade, Ana Brian, na *1ª Conferência Latino-Americana de Inteligência Artificial e Proteção de Dados*, a regulação para a proteção de dados pessoais está em marcha evolutiva no mundo, posto que 142 países já demonstraram instrumentos normativos sobre o instituto; ressalta que, o Regulamento Geral de Proteção de Dados (RGPD, 2016) da União Europeia é um exemplo de postura severa para esta proteção.

Como pode ser visto na imagem abaixo, os países que já possuem normatividade relativa ao tratamento de dados, encontram-se retratados na cor azul, o que revela que boa parte dos países do mundo, em todos os continentes, estão construindo normativas para regulação e proteção de dados sensíveis.

IMAGEM 1
PAÍSES COM REGULAÇÃO GERAL DE TRATAMENTO DE DADOS PESSOAIS



Fonte: Relatório da Fundação Getúlio Vargas (FGV, 2021) [19]

[19] O relatório é fruto da 1ª Conferência Latino-americana de Inteligência Artificial e Proteção de Dados, ocorreu no dia 1º de outubro de 2021, com participação de representantes do Ministério da Economia, da Fundação Getulio Vargas (FGV) e diversos pesquisadores da temática da Inteligência Artificial e Proteção de Dados.

Desses, 142 países possuem algum tipo de instrumento neste sentido, também já existem 94 países que instituíram a autoridade de proteção de dados, e o uso da internet alcançou 65% da população mundial, o que demonstra dinâmica importante na direção da proteção dos dados como direito fundamental.

No Brasil, a LGPD (2018) estabeleceu critérios de proteção significativa a pessoa física contra o impacto nos dados pessoais ou sensíveis, delineia em seu artigo 7º, inciso I, que o *tratamento*, ou seja, a manipulação de dados sensíveis somente poderá ser realizada mediante o consentimento do titular, mediante a boa fé e para alguns fins.

Inclusive, para coibir e dar força sancionadora a normativa trouxe sanções (vigentes somente a partir de setembro de 2020) de caráter administrativo, representando apenas multas e sanções administrativas, sem desmerecer aspectos positivos voltados à classe empresarial. Não obstante, conforme o artigo 52 da LGPD (2018), criou a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, que passou a integrar a Presidência da República, de acordo com o expresso no artigo 55-A.

Há, contudo, duas limitações importantes da LGPD (2018) que pode prejudicar a execução plena do texto constitucional no seu objetivo protetivo, que é a inaptidão para responsabilizar indivíduos cuja conduta esteja ligada ao cometimento de condutas de caráter penal e, também, no alcance dos crimes cometidos sob a forma extraterritorial, fora do território nacional, com ressalvas.

Nessas concepções, a lei geral de dados não se presta a prevenir a criminalidade tradicional ligada aos dados, mesmo sensíveis, nem mesmo no âmbito digital, posto que possui proibição expressa de aplicação no âmbito penal e da segurança pública, conforme apresenta o artigo 4º, prestando-se exclusivamente, as condutas relacionadas ao âmbito administrativo e cível.

> Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
>
> [...]
> III - realizado para fins exclusivos de:
> a) segurança pública;
> b) defesa nacional;
> c) segurança do Estado; ou
> d) atividades de investigação e repressão de infrações penais; ou
>
> IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei. (LGPD, 2018)

Tal aspecto permitiu uma lacuna importante que poderá ser suprimida por uma nova lei de caráter penal, ou mesmo, a partir da reconfiguração desta própria lei, contudo, esta crítica é necessária em razão da insuficiência desta LGPD (2018) pelo seu caráter cível.

É bem verdade que o Poder Legislativo já vem promovendo alguma modificação no Direito Penal brasileiro, visando reduzir a atipicidade dos crimes cibernéticos no ordenamento pátrio, em especial, incrementando o Código Penal (Decreto-Lei 2.848/1940), para o enfrentamento dos crimes por meio da internet, porém, diante da evolução tecnológica esta se demonstra ainda incipiente.

Os instrumentos existentes no Brasil resumem-se, no âmbito penal, a poucas normativas dispostas para proteção de dados da sociedade; assim, a Lei nº 12.737 de 30 de Novembro de 2012 (Lei Carolina Dieckmann) [20] foi marco inovador ao tipificar a invasão de computadores e violação de dados e divulgação (*hacking)* estabelecendo pela primeira vez, esta violação como crime próprio.

Defende Cavalcante (2020), que há atipicidade em muitos crimes cibernéticos que ocorrem no Brasil, mas não em todos, posto que alguns crimes impróprios, comuns, se praticados por meio de dispositivos podem ser alcançados pela normativa comum do Código Penal, a exemplo de um homicídio por meio de dispositivos eletrônicos, cujo desligamento de equipamentos pode ser alcançado do mesmo modo, em razão do resultado; também, do crime de racismo (por meio das redes) que pode ser acobertado pelo ímpeto sancionatório da Lei nº 7.716, de 1989.

Recentemente, alguns crimes (impróprios) do Código Penal foram reforçados pela Lei nº 14.155 de 27 de maio de 2021, com expresso aumento de pena a partir de dispositivos eletrônicos ou informáticos, fato ocorrido com os crimes de furto e estelionato, tornando-os específicos quanto à penalidade em razão do meio eletrônico empregado.

Há também no ordenamento pátrio brasileiro, normativa considerada de excelência e de significativo rigor quanto à realização por meio da internet, constante da proteção existente no Estatuto da Criança e do Adolescente (ECA), Lei nº 8.069 de 13 de julho de 1990, cuja redação a partir da Lei nº 11.829 de 2008, nos artigo 240 e seguintes, trouxeram tipificação criminal relativo aos crimes cometidos por meio da internet, mas, de modo específico com crianças e adolescentes.

[20] Em maio/2011 a atriz brasileira Carolina Dieckmann teve seu computador invadido por hacker (cibercriminoso) que cooptou fotos íntimas e exigiu R$10 mil para não publicá-lo na internet, porém, da recusa da atriz as fotos foram divulgadas nas redes sociais causando danos à privacidade. Houve acalorada discussão popular sobre a criminalização de tal conduta, culminando em 2012, na inclusão normativa do crime de invasão de computadores, violação de dados e divulgação no Código Penal.

Em razão da moderna normativa de enfrentamento aos crimes cibernéticos do ECA, Cavalcante (2020) informa que este estatuto é uma exceção a regra da atipicidade dos crimes cibernéticos, tendo sido construído por regra Federal de 2003, e atualizada na Lei nº 11.829 de 2008, teve a inclusão como crime, das condutas realizadas "*por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro" (*BRASIL, 1990), tipificando de modo expresso o emprego de cenas pornográficas envolvendo crianças e adolescentes.

Como contribuição acadêmica, note-se que há, também, o regramento relativo à proteção ao tratamento de informações do *banco de dados* no Código do Direito do Consumidor, Lei nº 8.078 de 11 de setembro de 1990, porém, das infrações penais constantes no art.61, não é retratado sanção sobre dados, na esfera penal.

Por tudo, há uma carência normativa no direito em razão do nível tecnológico crescente dos meios da criminalidade virtual e suas diversas estratégias para lesar a sociedade; as novas modalidades de fraudes cibernéticas, desafiam o ordenamento jurídico e demandam atualização constante e maior completude, como é possível observar nos crimes realizados no tráfego de dados (e não a partir de dispositivos eletrônicos) como por exemplo, ocorre no que o FBI (2022) denomina de *predador em linha* ou *"predator on line".*

Assim, a inaptidão da LGPD (2018) no âmbito penal é significativa, posto que não é uma lei especializada sobre a proteção de dados para responder aos incidentes envolvendo a criminalidade organizada no ambiente digital, sendo insuficiente para os objetivos traçados no texto normativo constitucional, na perspectiva penal.

Essa relação entre criminalidade e ordenamento traz a reflexão sobre a necessidade de equilíbrio na implementação das tecnologias oriundas da cibernética e a necessidade de evolução do direito para proteger a sociedade que constantemente é impactada pela ação criminosa que afeta a dignidade humana, de modo significativo, em especial, nessa nova dinâmica da vida digital.

3. CRIMES CIBERNÉTICOS E OS IMPACTOS NA SOCIEDADE DIGITAL

A tecnologia digital neste início de século XXI, apresentou tal nível de expansão no uso dos recursos da informação, da comunicação e do compartilhamento de dados no ambiente virtual, jamais vista na história da humanidade anteriormente apresentando muitas

vantagens mas também problemas que precisam ser resolvidos no processo evolutivo da sociedade.

Segundo Schwab (2019), a sociedade esta submetida a quarta revolução[21] industrial, ou ainda, a industria 4.0, que consiste no desenvolvimento e uso das tecnologias para compartilhamento de informações potencializadas pelo advento dos algorítimos matemáticos e seus novos empregos, na automação robótica e na inteligência artificial.

Fato que vem modificando definitivamente as relações sociais e negociais, mas que segundo o autor está em estágio ainda inicial, posto que é inimaginável conhecer o ponto final dessa nova vertente, que se fundamenta no âmbito virtual, a partir da internet.

Como Castells (2013), o ambiente de compartilhamento de dados da internet, absorveu características da sociedade tradicional, momento em que os conflitos e desafios que se reproduziam no meio físico comum, passou a ser também reproduzido no ambiente virtual, apresentando benefícios e problemas do âmbito das relações comuns.

Desta forma, a criminalidade se adaptou ao ambiente do ciberespaço, promovendo golpes econômicos, espionagem, roubo de segredos comerciais, industriais e institucionais para obter vantagens indevidas, seja no aspecto econômico quanto no aspecto político-ideológico. (CASTELLS, 2013)

Segundo Perrin (2005), o ambiente virtual permitiu o surgimento do fenômeno criminal cibernético que é a designação de modo amplo, dos problemas da criminalidade surgidos e promovidos no ambiente de rede mundial de computadores, a internet, afetando fortemente os dados das pessoas e instituições e, ocasionando verdadeira devassa na vida das pessoas.

Na mesma direção, evidencia Simas (2014, p.12), que o cibercrime se apresenta como um *"fenômeno da criminalidade informática [...], condutas violadoras de direitos fundamentais, seja através da utilização da informática para a prática de um crime, ou como um elemento do tipo legal de crime"*, notadamente, agora em meio virtual e não mais físico como no modelo tradicional.

Na explanação de Castells (2013), o crime tradicional passou por um ajuste no modelo de operar, saindo do âmbito físico com fronteiras bem delimitadas, para atuar diante das fragilidades do mundo etéreo da rede mundial de computadores, tendo por pano de fundo,

[21] Klaus Schwab (2018) refere-se ao que denomina de Quarta Revolução Industrial ou Indústria 4.0 – acrescenta que a sociedade está vivenciando o auge de descobertas ligadas a tecnologia disruptivas, desenvolvimento da automação robótica e da tecnologia da informação jamais vivenciada pela humanidade e, tendo por consequência, vantagens e perigos para a sociedade.

tecnologias cada vez mais sofisticadas ou ainda, disruptivas conectadas com o mundo negocial ou empresarial.

O objetivo de cometer crimes e angariar vantagens indevidas, através da internet, levou a ressignificação do crime, seja do ponto de vista territorial ou do *modus operandi*, seja através da atuação individual isolada ou através da associação organizada criminosa, altamente profissionalizada, em ambos os casos, desenvolvendo estratégias tecnológicas de ponta, para lesar pessoas, instituições e empresas por meio do ambiente virtual.

3.1 RESSIGNIFICAÇÃO DO CRIME NO AMBIENTE CIBERNÉTICO

O uso maciço dos dispositivos tecnológicos promoveu um ambiente de notável interesse dos criminosos (ciberdelinquentes) que passaram a utilizar da internet para promover golpes econômicos, espionagens, roubo de segredos comerciais, industriais e institucionais para obter vantagens indevidas.

Tal realidade impacta a economia das pessoas e das instituições, a partir da tarefa de manipular de modo desautorizado, os dados e as informações da sociedade através de meios fraudulentos, ressignificando a criminalidade, a partir de um novo ecossistema de compartilhamento de informações sem barreiras e globais.

Como resultado, pode-se observar que o cibercrime em dado momento auxilia e potencializa crimes preexistentes através do ecossistema da ciberdeliquência[22], como também está criando novas modalidades criminosas exclusivas do ambiente virtual, como a extorsão pelo sequestro de dados digitais (r*ansomware*), de pessoas e segredos industriais de empresas.

A potencialização dos crimes no âmbito cibernético vem contribuindo para novos movimentos das organizações internacionais terroristas, a partir do meio digital, fazendo surgir o denominado *terrorismo de baixo custo.* (SUAREZ; ACÁCIO, 2018).

O terrorismo de baixo custo consiste em ataques violentos, com mínima organização e requisitos técnicos facilitados pelo uso da internet, como o aliciamento de terroristas através de aplicativos[23], mensagens criptografadas que dificultam o rastreamento,

[22] Ciberdelinquência é a delinquência no ciberespaço. Disponível em https://www.infopedia.pt/dicionários/língua-portuguesa/ciberdelinqu%C3%AAncia?intlink=true acesso em 08/03/2022;

[23] O aplicativo Telegram, que tem um sistema de mensagens criptografadas tornou-se a plataforma preferida de membros do grupo terrorista conhecido como o *Estado Islâmico*, uma vez que plataformas como Facebook, Twitter e YouTube, possuíam maiores barreiras de censura para conteúdo violento. (SUAREZ; ACÁCIO, 2018).

liderança dos aliciados e ordens de execução de terrorismo, tudo de modo remoto e à distância, fato que reduz custos da operação terrorista. (SUAREZ; ACÁCIO, 2018).

Assim, enaltecem a necessidade de observar a adaptação das organizações internacionais terroristas a partir do início do século XXI, para uso de novos métodos digitais de cometimento do crime, atuando inclusive, de modo organizado e em concerto, através de reuniões virtuais em redes sociais.

Nesse contexto, a utilização combinada do corpo a corpo e os ataques com uso de armas de fogo e bombas, estão diminuindo ao longo dos anos, levando o planejamento do terrorismo a ser executado à longa distância, favorecendo o terrorismo de baixo custo, conforme retratado por Suarez e Acácio (2018); na mesma direção, a atividade delituosa passa a demandar enfretamento por meio de cooperação internacional séria, inevitavelmente.

Nesse contexto, acredita Lévy (1996), que no mundo virtual o compartilhamento dos dados em rede dificulta a distinção entre o que é público e privado, o que é comum do reservado, o que é direito subjetivo ou direito objetivo, levando essa inconsistência para a análise de bens e dos corpos, bem como, suas produções, o crime passou a atuar nesse ambiente em que não existem limitações e barreiras nem categorias específicas, relativizando tudo que se pode alcançar ou que esteja exposto na rede.

A partir desta concepção de falta de fronteiras físicas e limites para as relações no virtual, a cibercriminalidade passou a se valer da extraterritorialidade no cometimento do crime cibernético, sendo desafio deveras importante, visto que qualquer indivíduo, de qualquer lugar do globo, pode cometer fraudes no Brasil mesmo estando fisicamente em outro continente, e caso não haja conexão com outros indivíduos neste território pátrio, há total atipicidade de responsabilização criminal, ainda que os crimes cometidos sejam graves.

Este é um ponto de atenção que contribuiu para a ressignificação do crime tradicional para o ambiente cibernético, de modo definitivo, visto que o local de crime no qual as perspectivas geográficas como a sociedade a conhecia, foram totalmente desconstruídas, nesse modelo de criminalidade pulverizada no ambiente digital sem fronteiras.

Para melhor compreensão, as distintas limitações e fronteiras existentes nas relações do mundo físico tradicional deixaram de existir, as tecnologias lançaram à sociedade novos desafios a partir da interação à distância, por consequência, o Direito precisa se reestrutura para regular tais relações mesmo diante do advento dessa extraterritorialidade.

O grande desafio dessa discussão sobre a extraterritorialidade está justamente na relação do fato do criminoso atuar fora do espaço geográfico do Brasil, apesar de afetar estruturas internas do país, portanto, impossibilitando a responsabilização de criminosos pela

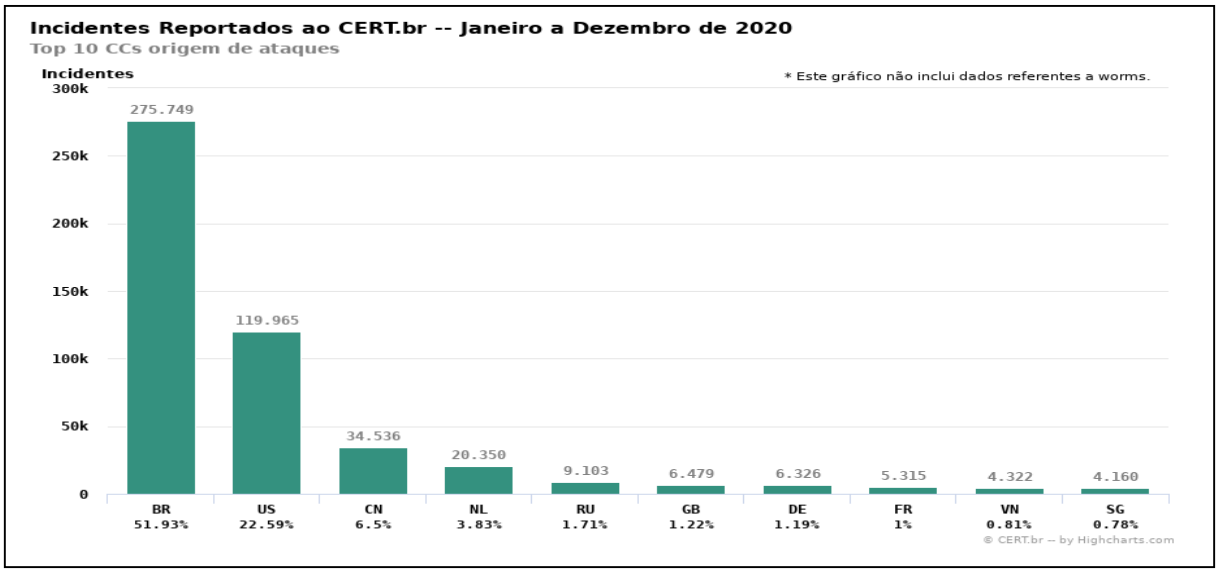
legislação pátria que somente pode alcançar quem está no território brasileiro ou quem atua com consórcio com outro que se encontra geograficamente no âmbito interno.

Para Marcel (2019) a perspectiva da extraterritorialidade é importante contexto a superar diante do cometimento de crimes no Brasil a partir de outros países ou continentes, é preciso conceber que o ambiente virtual precisa ser regulado e controlado sob novo tratado de direito, que considere tal questão envolvendo a expertise de outros Estados internacionais.

Há que analisar, entretanto, que o ambiente virtual *"como representa um conjunto global de redes de computadores interconectadas, não existe nenhum governo, organismo internacional ou entidade que exerça controle ou domínio absoluto sobre a internet*", fato que torna a tarefa de controle ainda mais difícil e dependente de cooperação internacional. (MARCEL, 2019)

Nesse contexto, como é possível analisar no gráfico 1, abaixo, os ataques contra estruturas informáticas no Brasil originadas fora do país, aproximou-se de 50% do total registrado em 2020, danos que pelo fato dos criminosos não se submetem ao ordenamento e à jurisdição brasileira, não puderam ser responsabilizados pelo caráter extraterritorial de atuação, fora do ambiente pátrio.

GRÁFICO 1
ORIGEM DOS ATAQUES CIBERNÉTICOS NO BRASIL – JAN A DEZ 2020 (TOP 10)



Fonte: CERT.br (2022)

Nesse contexto, 51,93% dos ataques cibernéticos entre janeiro e dezembro de 2020, foram originados em estruturas de internet do próprio Brasil, entretanto, a outra parcela originou-se a apartir de países distintos, de todos os continentes.

Assim, foram originados dos Estados Unidos da América (USA) 22,59% dos ataques que objetivaram gerar danos em estruturas informáticas no Brasil, seguidos dos geograficamente distantes: China (CN-6,5%), Noruega (NL-3,83%), Rússia (RU-1,71%), Gran Bretanha (GB-1,2%); Dinamarca (DE-1,19%), França (FR-1%), Venezuela (VN-0,81%) e outros, demonstrando de modo explícito, o desafio da extraterritorialidade diante da necessidade de cibersegurança[24] a ser desenvolvida no Brasil. (CERT.br, 2022)

Como reflete Marcel (2019), diante deste contexto, há entrave na responsabilização de usuários da internet e dificuldades legislativas existentes na atualidade, como a falta de normas legais específicas sobre a utilização de serviços disponíveis na internet e sobre a responsabilidade a eles inerentes, que permeiam tais discussões.

Assim, a regulação deve, por estas razões, se realizar no âmbito interno e soberano de cada país, pois a territorialmente gera a liberdade para estabelecer responsabilidades, contudo, não pode ser descartada a importância da cooperação internacional para limitar e desestimular a ação criminosa que age internacionalmente.

Confundem-se os juízes que, por vezes, tentam aplicar por *analogia* as normas gerais já existentes, para situações peculiares dos crimes digitais, isso quando não são céticos quanto a possibilidade de encontrar amparo legal nas normativas existentes, em virtude da ausência de uma legislação específica para a internet. (MARCEL, 2019)

Como retrata a Interpol (2020), faz-se necessário uma estratégia mundial contra cibercrimes, na qual os países membros devem reconhecer, antes de tudo, a importância de ações contra os delitos cibernéticos, o impacto financeiro e o uso terrorista da rede social.

Sendo necessário criar sistemas de detecção de ciberdelitos e identificação de delinquentes (inclusive, delinquência criminosa organizada), gestão de provas eletrônicas, análise forense digital, intercâmbio e análise de informações, atenção a evolução de ameaças e tendências, análise da correlação entre informação física e digital. (INTERPOL, 2020).

Nessa discussão, importante se faz enaltecer que o Brasil ainda não é signatário do *Tratado de Budapeste*[25], instrumento internacional dos quais países europeus, bem como, os Estados Unidos são signatários e que tem formalizado estratégias tecnológicas e jurídicas, pautadas na cooperação internacional e boas práticas, para o enfrentamento desta realidade criminosa cibernética.

---

[24] Cibersegurança - são técnicas de segurança realizadas para enfretamento do crime no ciberespaço;

[25] Tratado internacional realizado em Budapeste na Hungria (28 Abr 1977), com vigência desde 1980, sendo administrado pela Organização Mundial da Propriedade Intelectual, que possui 75 países signatários; o Brasil não realizou adesão, contudo, o governo federal em agosto de 2020 enviou mensagem ao Congresso Nacional para ser signatário deste documento internacional.

O Brasil, por sua vez, apesar de estar como *observador* do referido Tratado de Budapeste, ainda não aderiu efetivamente ao mesmo; postura que defende-se nesta pesquisa como relevante, em razão da importância dos institutos normativos que estão sendo construídos no âmbito cooperativo internacional.

No plano do ordenamento jurídico brasileiro, esta limitação por si só, em responsabilizar tais criminosos, torna-se mais um desafio a ultrapassar diante desse modo de operação criminal e traz dúvidas sobre como se daria a responsabilização de um indivíduo ou em associação criminosa, ao ferir normas internas de acesso ao ambiente virtual, estando ele fora da jurisdição física e soberana do estado brasileiro. (MARCEL, 2019)

Por serem transnacionais e sem fronteiras, organismos devem atuar cooperados em locais geograficamente distintos, para que tenham capacidade jurídica de enfrentar a ciberdelinquência, em sua estratégia de atualização tecnológica contínua.

Além da extraterritorialidade é também preciso responsabilizar indivíduos que cometem crime fora do país, e também, da necessidade de criar nas pessoas comuns, conhecimento suficiente e consciência sobre o uso do digital e, também, nas instituições jurídicas de que o digital precisa ser regulado pelo direito.

A problemática consiste, em superar a equivocada ideia de que a internet não pode ser regulada pelo direito de modo a promover a sua tutela, é imprescindível, entretanto, postura interdisciplinar para examinar aspectos da rede de computadores. (MARCEL, 2019)

Nos estudos de Vittorio Frosini[26] (1986), este destaca que a justiça precisa desenvolver *consciência tecnológica* para não permanecer inservível diante da problemática decorrente do digital, sendo necessário adotar postura reflexiva crítica e reativa.

Portanto, quando se pensar em constituir uma segurança cibernética ou cibersegurança *"prática que protege computadores e servidores, dispositivos móveis, sistemas eletrônicos, redes e dados contra ataques maliciosos."* (LIN e HERB, 2020); deve-se levar em conta a razão dos delitos de internet e a importância do direito de regular e criar estruturas de segurança a partir do direito.

Qualquer que seja a estratégia para coibir a cibercriminalidade em um país democrático deve estar fundamentada em várias linhas de ação, se apoiando nos esforços conjuntos de vários países.

[26] Vittorio Frosini é filósofo e jurista italiano considerado o *pai* dos estudos sobre a cibernética, atrelados ao ordenamento jurídico.

Não obstante, ampliar as capacidade de monitoramento e controle pelo Estado brasileiro sobre a utilização da internet, visando maior segurança da população, há que se ressaltar a importância dos limites na construção das estratégias e modelagem de cibersegurança e a prevenção de abusos, para que não se afete de modo negativo, a dignidade da pessoa humana que inicialmente se deseja proteger.

3.2 IMPACTOS DO CIBERCRIME NO BRASIL E NO MUNDO

A cibercriminalidade não é fenômeno novo, contudo, vem se expandindo em tamanha velocidade que tem trazido à tona a necessidade melhor compreensão de seu impactos visando melhor conceber soluções de enfrentamento.

Como visto, o advento da pandemia que impactou o globo a partir de março de 2020, elevou significativamente o uso dos recursos tecnológicos para o relacionamento social e para a resolução dos problemas do cotidiano, de sobremodo, fazendo aumentar com grande impacto o fluxo de dados na internet.

Como objetivo de distanciamento e restrições de deslocamento quase em escala global para evitar a propagação do coronavírus, boa parte da população mundial passou a se relacionar pela internet, fato que criou um ambiente favorável à vulnerabilidade dos dados das pessoas em rede, permitindo maior permissividade do ponto de vista da segurança, culminando na ação de cibercriminosos, em busca de vantagens indevidas.

Em pesquisa do Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (CETIC.br) que visou verificar o impacto da pandemia no modo como os brasileiros utiliza a internet, foi possível revelar que "*72% dos usuários de Internet procuraram informações ou realizaram serviços públicos on-line relacionados aos direitos do trabalhador ou previdência social, enquanto 20% fizeram consulta com médicos ou outro profissional",* ou seja, buscando informações na rede de computadores. (CETIC.br, 2020)[27]

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil [28] é um Grupo de Resposta a Incidentes de Segurança (CSIRT) de Responsabilidade Nacional, mantido pelo Comitê Gestor da Internet no Brasil (CGI), órgão responsável pelo monitoramento dos crimes cibernéticos no país visando melhoria da rede. (CERT.br, 2021)

[27] Cetic.br – dados disponível em https://cetic.br/pt/noticia/painel-tic-covid-19-apresenta-dados-ineditos-sobre-acesso-a-servicos-publicos-on-line-e-desafios-a-privacidade-durante-a-pandemia/. Acesso em 13 Abr. 2021;

[28] Descrição sobre CERT.br com missão, políticas e serviços pode ser encontrado no termo regulatório RFC 250 (conhecido como BCP 21) disponível em: https://cert.br/about/rfc2350/;

Não obstante, no momento de pandemia, em pesquisa realizada entre abril e maio de 2020, a INTERPOL (2020) ressaltou que o uso maciço da internet nessa ocasião, cuja interação física restava comprometida, possibilitou aos cibercriminosos um ambiente favorável para ampliação do cibercrime a partir das vulnerabilidades tecnológicas.

Revelou que muitas fraudes estavam relacionadas a existência de páginas falsas e links ligados ao tema *Covid-19* e link falsos ligados aos auxílios governamentais. Neste estudo da Interpol (2020)[29] ficou evidente que os crimes cibernéticos mais comuns cometidos durante o período de pandemia foram: roubo e sequestro de dados, acesso a informações essenciais e bancárias, construção de domínios malignos, utilização de softwares maliciosos, desinformação, links e correios eletrônicos falsos, utilização da rede para exploração sexual infanto-juvenil; não obstante, podem-se destacar também, os danos irreversíveis à propriedade intelectual, todas violações que se deram a partir do ambiente cibernético.

Corroborando com o aumento significativo dos crimes cibernéticos intrapandemia, o editorial da revista eletrônica Valor Econômico, retratou exatamente a mesma realidade, ao demonstrar pesquisa da IBM (*International Business Machines Corporation*).

> o monitoramento de eventos de segurança digital feito pela IBM, [...] em março, com a maior adoção do *home office*, houve aumento de 600% de envio de e-mails maliciosos na comparação com o mês anterior. 'foram tentativas de fraude [em quantidade] quase dez vezes maior de um mês para outro'". (TAUHATA; MOREIRA, 2020) [30]

Segundo relatório da IBM Security de 24 de fevereiro de 2021, o *Índice de Inteligência de Ameaças X-Force*[31], destacou que os incidentes cibernéticos cresceram em relação a 2020, tendo os cibercriminosos focados em lucrar com os desafios que a pandemia do Covid-19 apresentou; tendo havido uma concentração na falsificação de paginas de pedido dos benefícios assistenciais e emergenciais dos governos.

---

[29] A Interpol mantém uma rede de especialistas em ciberdelinquencia, com por pessoas especializadas na matéria oriundas dos países membros, de empresas privadas, organismos públicos e do mundo acadêmico, que fazem intercambio de informações e boa praticas contra delitos no âmbito cibernético. Essa pesquisa foi realizada durante a Pandemia do Sars Covid-19.

[30] V. Tauhata e Moreira (2020);

[31] Este índice da IBM se baseia em "*percepções e observações obtidas a partir do monitoramento de mais de 150 bilhões de eventos de segurança por dia em mais de 130 países. Além disso, os dados são coletados e analisados de várias fontes dentro da IBM"*..(IBM, 2021)

Segundo o estudo da IBM (2021) houve uma concentração de ataques a órgãos considerados vitais aos esforços globais contra o Covid-19 como hospitais, fabricantes de produtos farmacêuticos e médicos, empresas de energia, da cadeira de suprimentos relativos à prevenção da doença, pondo em alerta sobre questões envolvendo a sobrevivência de pessoas, em meio a crise sanitária.

Apesar de compreender com o pensamento de que já havia um movimento de aumento de ocorrência de cibercriminalidade mesmo antes da pandemia, há de compreender que o período intrapandemia elevou consideravelmente a ocorrência desses crimes.

Não obstante, o relatório da *Risk Based Security,* outra pesquisa da Kaspersky Security Network em 2019, já registrava a exposição maciça dos dados sensíveis de usuários desde aquele período, como destaca:

> um número impressionante de 7,9 bilhões de registros que foram expostos por violações de dados somente nos primeiros nove meses de 2019. Este número é mais que o dobro (112%) do número de registros expostos no mesmo período em 2018. (KASPERSKY, 2019)

Na América Latina, segundo relatório de ameaças demonstrado pela Kaspersky (2020)[32], o Brasil está entre as nações mais vitimadas da cibercriminalidade, apresentando-se como líder absoluto de ataques cibernéticos na ordem de (56%) dos casos totais, seguido do México (28%), Peru (5,4%), Colômbia (7,3%), Argentina (1,9%) e Chile (1,6%).

Os recentes dados de abril/2021, revelado pela Mcafee (2021 p.11), ressalta que o interesse atual são os dados armazenados em "nuvem", sendo que mais de 3 milhões de ataques a nuvens ocorreram, tendo vulnerabilizado e agregado dados de mais de 30 milhões de usuários da *McAfee MVISION Cloud*, o Brasil apareceu com relevância no terceiro e quarto trimestre de 2020, ficando em terceiro mais invadido do mundo.

Estes armazenamentos em nuvem continham dados privados coletados de diversas áreas como serviços financeiros, varejo, tecnologia, instituições públicas, educação, jurídico, saúde, setor imobiliário, transporte comércio, entre outros. (MCAFEE, 2021, p.11) [33]

---

[32] KASPERSKY. Em ano de pandemia, cibercrime mira as empresas. 29 set 2020. Disponível em https://www.kaspersky.com.br/blog/pandemia-cibercrime-mira-empresas-america-latina/16090/ ;

[33] MCAFEE *Labs Threats Report* (Mcafee Labs: Relatório de ameaças). April 2021. Disponível em https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-apr-2021.pdf acesso em 21/05/2021.

No panorama mais recente, o *Relatório Fast Facts* da Trend Micro (2021) revela que o Brasil é o segundo país mais acometido por software malicioso do tipo *ransomware,* por ficando atrás apenas dos Estados Unidos da América (EUA).

Nessa mesma direção informa que o cenário de ameaças para 2022, não será tão fácil e defende a implementação de estratégias de segurança, ao passo em que informa que algumas das principais ameaças estarão relacionadas a ameaças em nuvem, entre outras. (TREND MICRO, 2022)

Permanecem igualmente, as ameaças inerentes aos *ransomwares* utilizados para sequestro de dados e pedidos de resgates por criminosos cibernéticos, exploração de vulnerabilidades do ambiente, ataques ligados às *commodities*, ameaças a partir das tecnologias disruptivas como a internet das coisas (IoT) domésticas, além das ameaças ligadas a cadeia de abastecimento e serviços essenciais da sociedade. (TREND MICRO, 2022)

Para o *Federal Bureau of Investigation* (FBI, 2022), agência federal de segurança dos Estados Unidos da América (EUA), a atividade cibernética possui malícia capaz de ameaçar a segurança do público em geral, da segurança nacional e econômica da nação; vez que os crimes são rapidamente adaptados às vulnerabilidades do sistema, intensificando os ataques à infraestrutura de nuvem crítica com abordagens novas e sofisticadas.

Formas de se prevenir de tais ameaças pairam sobre políticas rigorosas de gerenciamento de segurança cibernética no uso da internet, fechamento de redes para grupos específicos e controle de acesso, fortalecimento do servidor e robustez dos sistemas informáticos corporativos, com forte investimento em segurança cibernética.

Também, se faz necessário além dos investimentos, o aprendizado pelo usuário em fazer bom uso da rede, haja vista, parte das vulnerabilidades serem ocasionadas pela engenharia social de quem acessa o ambiente cibernético.

Contudo como demonstra o relatório de *Sensação da Segurança Digital SMB 2022*, publicado pela ESET (2022), após entrevistar 1.200 tomadores de decisão sobre segurança cibernética de *pequenas e médias empresas*, há uma crescente preocupação sobre as implicações dos ataques com a perda de dados, impactos financeiros, perda de confiança do mercado e do cliente, posto que os investimentos significativos, nem sempre estão se refletindo em qualidade de proteção.

A pesquisa revelou sobre a ineficiência dos investimentos realizados em segurança cibernética por boa parte desses empresários, sendo que 70% dos representantes, admitiram que os investimentos nessa modalidade de segurança digital, não acompanhou as mudanças e modelos operacionais dos ataques. (ESET, 2022)

Na mesma direção, segundo a Akamai Technologies empresa de segurança cibernética mundial e de segurança em nuvem, entre abril de 2021 e setembro de 2022 (aproximadamente 18 meses), o comércio digital no Brasil, *e-commerce*, registrou mais de 162 milhões de ataques, na maioria do tipo *web apllication*, que se resume no acesso a réplica sobreposta de páginas de sites originais, criadas por criminosos. (CISO ADVISOR, 2022b)

Ao inovar e se adaptar continuamente por meio de novas ferramentas de inteligência artificial, os criminosos cibernéticos desenvolvem novos vetores de ataque mais sofisticados e eficazes, que amplificam as metodologias criminosas anteriores, gerando uma autoevolução contínua perigosa, fenômeno que tem demonstrando a potencialização desse modelo de criminalidade, com os recursos da inteligência artificial e significativo potencial tecnológico de gerar danos a sociedade, como veremos a seguir.

4. INTELIGÊNCIA ARTIFICIAL E SEUS RISCOS: A NOVA PEDRA FILOSOFAL

A inteligência artificial possui um enorme espectro de questões complexas e ferramentas técnicas que demandam conhecimentos específicos da Ciência da Informação para melhor compreensão pormenorizada de seu funcionamento, este aspecto peculiar, desemboca em conhecimentos restritos que por vezes focam em questões técnicas, matemáticas e eletrônicas de comunicação e limitam a discussão sobre tais tecnologias.

Diferentemente desta dimensão, o objeto desta pesquisa submerge do ponto de vista epistemológico e construção de conhecimento a partir de um modelo transversal que analisa e discute as tecnologias de inteligência artificial e seus algorítmos, com a Ciência do Direito, focando na íntima interface dessas aplicações e seus impactos nos diversos ramos jurídicos, tornando-se desafio para os atores do direito estabelecer soluções para os problemas que afetam a sociedade, a partir do emprego dessas novas tecnologias.

Não se pretende esgotar neste trabalho, contudo, qualquer perspectiva de discussão sobre tais impactos, e sim, iniciar uma trajetória discursiva que possa coadunar a analise técnica sobre a inteligência artificial e os impactos sociais e jurídicos que esta acarreta na comunidade pátria e global, portanto, enaltecendo a temática como pedra filosofal do atual momento tecnológico que não pode sob qualquer pretexto econômico se distanciar do social.

Não obstante, ter o intuito de desenvolver aspectos positivos para a população os estudos que favoreceram as primeiras descobertas nos estudos da cibernética e da computação,

que envolviam necessidade de comunicação com os atributos da supercondutividade e transferência de informações eletrônicas, desenvolvidas inicialmente nos estudos de Turing (1950), retratado na obra *Computing Machinery and Intelligence*[34] (Máquinas de Computação e Inteligência), algo de negativo, surgiu com tais tecnologias.

O avanço das técnicas empregadas para o aprendizado das máquinas, formaram ao longo do tempo um conjunto de estímulos sistemáticos a existência deste tipo artificial de inteligência, que se apresenta, superevoluído, atualmente. Nessa direção, retrata Castro Júnior (2009, p.22/23) que o desenvolvimento informático contribuiu para a consolidação da IA a partir do incremento dos circuitos eletrônicos, contudo, sem qualquer foco social.

Muitos dos quais, baseados em carbono e silício, permitiram a criação de redes neurais, computação quântica, condutividade em grande nível, desenvolvimento de nanotecnologia[35] e algorítimos, que favoreceram o surgimento de máquinas capazes de realizar tarefas melhores que as desenvolvidas por seres humanos. (CASTRO JÚNIOR, 2009)

O estudo da robótica por *Kismet e My Real* desde a década de 30, levou a criação de máquinas capazes de expressar emoções simulares à humana, através da interconexão de subsistemas complexos; resultando na quebra de paradigma com reflexos no Direito, a exemplo da discussão sobre a personalidade jurídica dos robôs. (Castro Júnior, 2009)

Mas, segundo Bomfim e Gimenéz (2020a), foi na década de 50, que houve uma intensificação nas reflexões e compreensões a cerca das tecnologias que envolviam o aprendizado de máquinas e tais tecnologias da computação, como desdobramento dos estudos científicos de pesquisadores como *Hebert Simon, Allen Newell e John Mc Carthy*, que se debruçaram sobre esta temática, até então.

4.1 ASPECTOS CONCEITUAIS E IMPLICAÇÕES DA INTELIGÊNCIA ARTIFICIAL

O termo *inteligência artificial* empregado por McCarthy em 1956, durante a Conferência de Dartmouth na Inglaterra, passou a ser referência de avançada tecnologia; a criação de um sistema capaz de buscar informações orientado por algorítimos matemáticos, a partir de uma sequência de procedimentos ordenados, demonstrou capacidade da máquina de

[34] O clássico livro de Alan Turing demonstra os experimentos iniciais sobre computação e o aprendizado de máquina, conhecidos como "*Os testes de Turing"*. (TURING, 1950)

[35] Refere-se a objetos que encontram-se em tamanho microscópico ou em "*escala nanométrica, aplicada freq. à produção de circuitos e dispositivos eletrônicos com as dimensões de átomos ou moléculas".* Dicionário Oxford Languages. Disponível em https://languages.oup.com/google-dictionary-pt/ Acesso em 24 Abr. 2022.

resolver problemas (BOMFIM; GIMENÉZ, 2020a); refletiu a inteligência da máquina artificialmente criada para a realização de tarefas, de modo a *superar* o ser humano.

Segundo Hartmann Peixoto (2020), possui a IA a possibilidade de auxiliar em diversas tarefas como: reconhecimento de padrões; identificação de consistências e inconsistências a partir de determinada racionalidade; ampliar o aproveitamento de informações; incrementar organização de estratégias e permitir registros confiáveis para sistemas de controle (*accountability)*, portanto, sendo positivo em diversas aplicações.

Do ponto de vista cognitivo e visando discutir as implicações da Inteligência Artificial na contemporaneidade, conforme expõe Felipe Bomfim e Marta Gimenéz (2020b), há na busca da definição sobre inteligência, duas explicações gerais.

A primeira explicação é que inteligência está ligada ao ato de aprendizado enquanto capacidade de conhecer sobre algo e, na segunda, de modo *lato sensu,* compreende a capacidade de resolver problemas e conflitos, incluindo, a capacidade de adaptabilidade às situações imprevistas. (BOMFIM; GIMÉNÉZ PEREIRA, 2020b)

Evoluindo para análise da inteligência artificial, a pretensão do ato de pensar articulado com representações construídas *artificialmente,* a partir da interação entre programação para o aprendizado de máquina e a composição com dados comportamentais humanos, possibilitou o aprendizado de condutas a partir de dados levando ao desenvolvimento da IA, a partir do cruzamento de dados computacionais sofisticados.

Na concepção de Juli Ponce, revela que são sistemas com complexidades diversas dos mais simples aos mais sofisticados:

> El término inteligencia artificial, sistemas que manifiestan un comportamiento inteligente, pues son capaces de analizar objetivos específicos, Estos sistemas pueden consistir en un simple programa informático por ejemplo motores de búsqueda o sistemas de reconocimiento facial o de voz, pero también pueden estar incorporados en dispositivos de hardware, como robots o automóviles autónomos. (PONCE, 2019, p.2)[36]

Ademais, a inteligência artificial passou a se manifestar das mais variadas formas no ambiente da internet e dos negócios, por meio do reconhecimento facial e atividades

[36] Tradução livre: "O termo inteligência artificial, são sistemas que manifestam comportamento inteligente uma vez que são capazes de analisar objetivos específicos, esses sistemas podem consistir em um simples programa de computador, por exemplo, mecanismos de busca ou sistemas de reconhecimento facial ou de voz, mas também podem ser incorporados a dispositivos de hardware ou físico, como robôs ou carros autônomos." (PONCE, 2019; p.2)

autônomas, a exemplo dos equipamentos com autonomia de uso como, robôs, drones, entre outros. (BOMFIM; GIMÉNÉZ PEREIRA, 2020a)

Indo além da dimensão mais material, o conceito recente abarca também aspectos do pensamento e inteligência humana utilizados pela tecnologia, como nos informa o Conselho Nacional de Justiça do Brasil (CNJ, 2020) ao definir que a Inteligência Artificial, é um conglomerado de *"dados e algoritmos computacionais, concebidos a partir de modelos matemáticos, cujo objetivo é oferecer resultados inteligentes, associados ou comparáveis a determinados aspectos do pensamento, do saber ou da atividade humana*"; comporta, portanto, uma visão extensiva destes recursos.

Não obstante, como nos alerta Castro Júnior (2009, p.60), há uma *impossibilidade* da máquina computacional funcionar como um cérebro humano que possui a característica de utilizar a intuição, diferentemente da formalização de procedimentos, que é realizada pela máquina; segundo o autor é importante reconhecer que sempre haverá um conteúdo humano que matematicamente *não será possível acessar*, que não será conhecido, e portanto, incapaz será de ser compreendido pela máquina na sua atividade autônoma.

Superada *a priori* esta preocupação inicial, a inteligência artificial pode apresentar enorme sofisticação e mesmo assim, influenciar o processo decisório do ser humano, conquanto, atualmente, há diferentes e cada vez mais avançados tipos de tecnologias de IA.

Como revela Da Silva (2020, p.41), é possível observar *"assistentes pessoais com capacidade de entendimento de fala, buscadores, sistemas de recomendações, sistemas de apoio a decisões nas áreas de diagnóstico por imagens, de classificação de textos jurídicos".*

O incremento do mapeamento automático solos e o auxílio na estruturação das tecnologias disruptivas, usadas, por exemplo, na direção autônoma de veículos automotores (DA SILVA, 2020); bem como, na internet das coisas (IoT) existente em muitos equipamentos domésticos, são avanços relevante para o *conforto social.*

Como preocupação, nos alerta Ferrer (2021, p.293), que os tratamentos massivos de dados sensíveis por meio da técnica de *big data*, permitem a coleta de muitas informações adquiridas de modo oculta, através de padrões que superam os meios tradicionais de sua coleta, sendo possível analisar grande quantidade de dados capturados durante a utilização de assistentes domésticos como o *Siri* e a *Alexa*[37]*,* equipamentos ligados disruptivos e residenciais, que captam invasivamente dados sem consentimento dos usuários.

[37] *Siri e Alexa* são aparelhos lúdicos, mas tecnicamente são sintetizadores de linguagem e comunicação que quando conectados a internet possuem a capacidade de captar e transferir dados sensíveis dos usuários, podendo

Deste modo, o estabelecimento dessa dinâmica no uso computacional para o âmbito doméstico, penal, da saúde, do trabalho e na resolução do problemas cotidianos, nem sempre reflete o significado do *bem-estar social,* gerando uma dicotomia entre *conforto e bem-estar*, na discussão sobre aplicação da inteligência artificial, julgando-se necessário melhor avaliação dos riscos sobre tais aplicações.

Do ponto de vista da Teoria do Capital Humano sobre as relações trabalhistas, pôde-se observar que a IA não apresenta somente pontos positivos à sociedade, e que além de ser voltada para os processos, mercadorias e serviços, reflete uma mudança significativa de paradigma no uso do ambiente digital, em especial, no modo de produzir renda e economia no âmbito social, intervindo por vezes de modo negativo no mundo do trabalho (BOMFIM; GIMÉNÉZ PEREIRA, 2020a); ocasionando a perda de postos de trabalho.

Da análise do arcabouço jurídico brasileiro e da forma como a Inteligência Artificial está sendo implementada e gerida no Brasil, o que se observa é que existem muitas carências precisam ser discutida sobre a temática, e a Ciência do Direito e os instrumentos regulatórios precisam ainda serem aprimorados para o equilíbrio no uso dessas tecnologias.

Apesar do Brasil ser considerado um país bastante inovador na implementação das tecnologias de inteligência artificial a exemplo de reconhecimento facial, localização por GPS, robotização no Poder Judiciário, cadastro digital e conectividade para serviços através das plataformas governamentais, observa-se que há carência na perspectiva do direito formal.

O atual e crescente uso da inteligência artificial pelas pessoas privadas e pelo próprio Estado, não vem sendo tema de discussão junto a sociedade civil, de modo robusto, que permita construção eficaz do controle e regulação dessas tecnologias, em especial, diante das aplicações de monitoramento da população e emprego na segurança publica, a exemplo do uso para fins de política criminal ou penal.

Visando reduzir tais vulnerabilidades, o Brasil aprovou o Projeto de Lei (PL) nº 21-A de 2020[38], *"estabelece fundamentos, princípios e diretrizes para o desenvolvimento e a aplicação da inteligência artificial no Brasil*", contudo, surgido após o impacto da superconectividade pandêmica e da criminalidade cibernética, existe um atraso desta discussão junto a sociedade civil, que revela, também, certa imaturidade sobre este conteúdo.

Não obstante, segundo esse PL brasileiro, em seu artigo 2º, está expresso:

---

estabelecer perfiz personalizados a partir da voz, percepção de sentimentos e humor, biometria, além de realizar georreferenciamento.

> considera-se sistema de inteligência artificial o 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 predições, recomendações, classificações ou decisões, e que utiliza, sem a elas se limitar, técnicas como:
>
> I – sistemas de aprendizagem de máquina (machine learning), incluída aprendizagem supervisionada, não supervisionada e por reforço;
>
> II – sistemas baseados em conhecimento ou em lógica;
>
> III – abordagens estatísticas, inferência bayesiana, métodos de pesquisa e de otimização.
>
> Parágrafo único. Esta Lei não se aplica aos processos de automação exclusivamente orientados por parâmetros predefinidos de programação que não incluam a capacidade do sistema de aprender a perceber e a interpretar o ambiente. (BRASIL, 2020)

Não obstante, o início normativo, há algo importante a compreender nessa dinâmica, primeiro é compreender que os países mais pobres não possuem empresas de grande porte, como é o caso do Brasil que está em desenvolvimento, diferentemente das grandes nações como os EUA e China, com suas *Big Techs* e dinheiro para investir.

Note que empresas como o *Google, Facebook, Amazon, Microsoft, Baidu, Alibaba e Tencent,* que dominam atualmente o mercado digital e os investimentos em IA, por vezes, se autorregulam e inviabilizam o desenvolvimento da IA que considerem seus riscos e maior controle Estatal; do mesmo modo, que no âmbito do trabalho, inviabilizam um ambiente favorável a outros modelos econômicos que favoreçam o plano social, para além da econômica. (BOMFIM; GIMÉNÉZ PEREIRA, 2020a).

Cabe então ressaltar, que o Brasil caminha quanto a IA de modo positivo para uma regulação sob a dimensão legislativa, contudo, carece da discussão pormenorizada por parte da sociedade civil sobre todos os riscos envolvidos no uso das máquinas inteligentes, diante das muitas mazelas que surgem sobre as discriminações algorítmicas do sistema.

Da violação indiscriminada e automatizada dos dados sensíveis das pessoas por meio dos sistemas de inteligência artificial e seus algorítmos, ou mesmo, do emprego de tecnologias preditivas como recurso do sistema criminal brasileiro, discussões que necessitam ser amadurecidas, de modo urgente, no plano social.

4.2 INTELIGÊNCIA ARTIFICIAL E OS RISCOS À DIGNIDADE HUMANA

O Direito é importante instrumento de frenagem e contrapeso para o equilibro do desenvolvimento sustentável da tecnologia, para que esta não se distancie da lógica de proteção do Estado Constitucional Democrático, ampliando benefícios e eliminando malefícios, diante da ruptura e quebra de paradigmas que a cibercultura e a inteligência artificial já constituiu no modo de vida das pessoas.

Merece destaque que muitos riscos que se apresentam na análise da inteligência artificial, vão além da afetação da teoria do capital humano e meras consequências simplórias quanto aos dados sensíveis e privacidade, sinalizando que precisam ser melhor conhecidos, discutidos e regulados, não obstante, representarem uma probabilidade não certa de ocorrer.

Nessa concepção, não há uma definição específica sobre o que seria um *risco da inteligência artificial*, portanto, para fins acadêmicos tomar-se-á as definições de risco ligadas aos processos organizacionais do mercados de negócios e do mundo das finanças, de modo a aproximar a compreensão do leitor sobre essa perspectiva na IA.

Assim, em uma percepção geral, o risco apresenta-se como um tipo de incerteza que pode ser medida e mensurada antecipadamente, contudo, na visão de Assaf Neto *(*2015, p.158) *"risco pode ser entendido como a probabilidade de perda em razão de uma exposição[...]";* logo, há a possibilidade de prejuízo caso o risco de fato ocorra.

Na mesma direção, sob a ótica de Dias (2008, p.23) risco se apresenta como uma "*possibilidade, ou seja, trata-se de algo que existe e pode ocorrer, mas isso não quer dizer que sua ocorrência seja líquida e certa*", deixando claro, que há uma possibilidade de que se concretize de fato ou não, dependente de meios preventivos para mitigar possíveis efeitos.

Nesse sentido, os riscos apresentados nesta pesquisa são meramente exemplificativos, não abrangendo a totalidade de riscos existentes sobre a inteligência artificial em todas as áreas, seja pela dinâmica das diversas ciências e em razão das novas pesquisas e evolução tecnológica, que tem o condão de naturalmente ampliá-los.

Ademais, apesar da discussão sobre existir a probabilidade ou não de ocorrência desses riscos no plano fático, é importante ressaltar que à exceção de alguns poucos riscos que ainda estão sendo delineados pelos estudos científicos em andamento, a maioria desses riscos explanados, já se efetivaram de verdade na sociedade seja em maior ou menor proporção.

Notadamente, trazendo preocupação a sociedade em razão da velocidade e do impacto com que tais vulnerabilidades estão ocorrendo na vida das pessoas, que na maioria ainda desconhecem os efeitos nocivos da inteligência artificial, no plano fático.

Assim, como meio de discernir sobre a esta dinâmica à qual a sociedade está submetida, apresenta-se sem intenção exaustiva, mas sim, revelando um rol exemplificativo de

riscos, os principais aspectos de preocupação social a partir do emprego da inteligência artificial na atual dinâmica social, como será exposto.

4.2.1 Riscos inerentes à impossibilidade de responsabilização

a) Risco de Irresponsabilidade Civil

Como primeiro ponto, diversas organizações passaram a monitorar de modo contundente o hábito de consumo e comportamental de seus clientes nas redes sociais, bem como, como interagem com as respectivas plataformas de consumo com vistas a criar perfis de consumo, objetivando maior lucratividade sem responsabilidade com os efeitos sociais.

O acesso a bases de dados tornaram-se estratégias comerciais de diversas organizações, posto que como já delineado, os dados sensíveis dos clientes passaram a se apresentar como informações importantes no processo de persuasão das empresas, provocando o consumo de seus clientes. (GUERRA e TARGINO, 2021)

Na perspectiva da ciência de dados, tais estratégias de captação de dados dos consumidores e da população em geral, através das diversas plataformas de interação social através da internet, interconectando desejos, perfis, padrões de acesso e consumo.

Este acesso permite um ecossistema permissivo de compartilhamento, levando a uma irresponsabilidade consentida e justificável enquanto estratégia de marketing comercial oriunda de negócios empresariais, não obstante, ferindo de sobremodo o consentimento dos usuários no modo como os dados pessoais são manipulados, sem as limitações adequadas e com grande aporte abusivo tendo efeitos nefastos a sociedade.

As práticas irresponsáveis de grandes empresas de tecnologias, *Big Techs,* com dispoe de grande poder econômico e empregam altos investimentos em inteligência artificial, torna-se preocupante ao disseminarem práticas abusivas de marketing, criação de perfis de usuários e manipulação de informações sensíveis visando a cadeia de lucro.

Ademais, por vezes, atuando através de espiões cibernéticos e especialistas corporativos para angariar informações privilegiadas, demonstram como de modo silencioso e sem fiscalização, as empresas estão a captar dados e a violar privacidades, burlando a segurança digital e o livre consentimento, ou mesmo, a livre autonomia das pessoas, fragilizando de modo extensivo a sociedade, que está totalmente alienada sobre a atuação tecnológica dessas empresas e sobre como buscar a responsabilização dessas organizações.

Diante de tal realidade, é necessário separar e discernir o que são praticas aceitáveis de marketing e comércio que se coadunem com o Direito do Consumidor, e o que é abusivo e

fere o Direito Constitucional a Proteção de Dados Sensíveis, haja vista, a carência técnica e de fiscalização dos entres estatais diante da complexidade desta temática e dos investimentos cada vez maiores pela empresas em novas técnicas de persuasão econômica.

Para fins acadêmicos, convém analisar o lado perigoso dessas tecnologias com *foco no lucro* e não no bem estar social, a partir do exemplo de violação e manipulação abusiva de dados realizada pela empresa *Facebook ou Meta*[39]**,** cujas denúncias levaram seu proprietário a ser processado pelo Senado e Congresso Nacional dos Estados Unidos.

O *Facebook/Meta* foi acusado de utilizar inteligência artificial para atividades nocivas que visavam manipular as decisões das pessoas, com marketing agressivo e direcionamento discussões de ódio para criar engajamento populacional à rede. (SENADO DOS ESTADOS UNIDOS, 2018)

Não obstante, ter alcançado valor de mercado de U$1 trilhão de dólares, e sendo, reconhecidamente, uma das maiores redes sociais do mundo, as denúncias contra o *Facebook* levam o bom leitor a reconsiderar o lado negativo dessas aplicações, diante da fragilidade que impõe as pessoas comuns no uso, inocente e desavisado das redes sociais.

A jurisdição nessa experiência teve a necessidade de investigar violações relacionadas à privacidade de dados, segurança dos dados em razão dos constantes vazamentos de informações e compartilhamento de plataformas e as práticas abusivas do da empresa no tocante a proteção do consumidor.

O Senado dos EUA teve a necessidade de reunir dois Comitês com 44 pessoas para a investigação, a *Comissão de Comércio, Ciência e Transporte* e a *Comissão do Judiciário*, ambas, emitindo relatório robusto sobre o *case* desta *bigh tech* e tendo comprovado a maior parte das denúncias.

É importante salientar que em razão das diversas denúncias que macularam a imagem da empresa, o Facebook modificou seu nome de fantasia e passou a ser denominado de *Meta*, reformulando a identidade empresarial.

Acredita-se, em razão das polêmicas sobre a quebra de privacidade de dados, além da moderação inadequada e discriminatória de conteúdos, que culminou com investigação do Senado e Congresso dos Estados Unidos em face do proprietário Marc Zuckerberg. (SENADO DOS ESTADOS UNIDOS, 2018)

---

[39] A Empresa *Facebook* passou a se chamar *Meta.*

Nesse sentido, o Senado dos EUA (2018) analisou processualmente as seguintes denúncias contra o Facebook/Meta[40]:

> - afetação da saúde mental de adolescentes, ao desencadear situações de insatisfação com a autoimagem e favorecendo o suicídio; cuja identificação por funcionários, foi propositadamente desconsiderada pela cúpula gestora da empresa;
>
> - atuação de modo agressivo com publicidade para engajar crianças a partir de 6 anos de idade, que foi suspenso; além de táticas para pré-adolescentes, evitando a adesão desse público a rede concorrente; a empresa orçado para o público infantil R$ 2,1 bilhões de reais, para investir no engajamento de menores de 18 anos;
>
> - manipulação de algorítmos dos espaços de discussão política, favorecendo *cancelamentos* de pessoas de determinado seguimento e preterindo outros;
>
> - estabelecimento de regras nas plataformas que autorizavam pessoas com maior poder aquisitivo e agentes políticos a ter maior liberdade, mesmo agindo de modo abusivo;
>
> - aplicação de inteligência artificial para moderação de conteúdos, que, contudo, somente removeu apenas 3% a 5% de materiais com *discurso de ódio* e 0,6% de *violência;* e na qual *troca de tiros* e *acidentes com veículos*, eram rotulados como jogos de *paintball.*
>
> - omissão da plataforma no tráfico de mulheres do sudeste asiático aliciadas através de anúncios de trabalho para trabalho doméstico no Oriente Médio; cuja descoberta não teve intervenção da empresa;
>
> -favorecimento de grupos políticos específicos durante as eleições dos EUA, promovendo publicidade direcionada a deturpar o processo decisório dos cidadãos;
>
> -intensificou a desinformação sobre conteúdos políticos, de modo crônico;
>
> -direcionou conteúdos de incitação a violência, discurso de ódio e de organizações criminosas direcionados a países como o Brasil, índia, Egito, Turquia e Filipinas, diferentemente, dos Estados Unidos e Europa Ocidental, estimulando aumento da violência;
>
> -disparou conteúdos de baixa qualidade e tóxicos para *viraliza*r, favorecendo os anúncios de marketing, cujos conteúdos com animosidades, que não foram removidos;
>
> -usou algorítmos racistas e embasados no ódio, fator que pode ter contribuído para agravar crises em todo o mundo; nos quais os alertas de funcionários, não foram atendidos.

[40] Em novo escândalo conhecido como "*Facebook Papers"* ocasionado pelo testemunho da delatora e ex-gerente de produto do Facebook Inc., Frances Haugen, perante o Comitê do Senado dos EUA sobre Proteção ao Consumidor, Segurança de Produtos e Segurança de Dados, em 5 de outubro de 2021, esta denunciou que a empresa reconhece que algumas tecnologias causam danos aos usuários, mas que os ignoram como cultura, posto que consideram mais o lucro do que a segurança dos usuários do *facebook e instagram*, mesmo as crianças, logo, colocando o lucro em primeiro lugar. (KOLAKOWSKI, 2021)

> - estimulou a disseminação de desinformação e estimulou brigas entre as pessoas na rede, para gerar polarizações e engajamento;
>
> - não reconheceu os discursos de ódio oriundos dos países Árabes, alegando que havia poucos moderadores humanos que sabiam falar aquela língua; na Índia, as plataformas tiveram os discursos de violência ampliados, quando o país passava por grave instabilidade;
>
> -apresentou divergências diversas sobre os efeitos nocivos da quebra da privacidade, dos dados e na captação de biometria, voz e geolocalização dos usuários com o uso da inteligência artificial e algorítmos;
>
> -demonstrou total insensibilidade na gestão dos algorítmos discriminatórios e estímulos ao suicídio dos jovens, quando os funcionários teriam se manifestado contra a pura política do lucro da empresa.

Diante de tal dimensão abusiva como no caso denunciado sobre o Facebook/Meta, o Direito pode e deve ser instrumento acessível para a sociedade para estabelecer regras que funcionem como instrumento de frenagem às tais práticas dessas grandes empresas, tornado-se suporte *vivo*, de imprescindível importância diante das tecnologias de inteligência artificial.

A fim de coibir o abuso de poder de organizações como as reveladas anteriormente tratou o Parlamento Europeu de gerar normativa preventiva importante, sendo destacada por Ferrer (2021, p.294), como importante instrumento normativo que culminou com o Regulamento Europeu nº 679/2016.

Em reflexão comparativa, o regulamento permitiu a discussão sobre as limitações dos criadores e implementadores de inteligência artificial, e ampliou o exercício do direito pelos usuários, perante os responsáveis e tratadores de dados. (FERRER, 2021)

Segundo o RGPD (2016) europeu, a frenagem das ações abusivas se dá pela possibilidade do usuário exigir direitos de acesso, de informação e de reclames junto aos órgãos que compõe a autoridade de dados e aos órgãos jurisdicionais da Europa, além da sistemática que restringe o uso da automação de modo indiscriminado, conforme o art. 22.

Como retrata o artigo 15, do RGPD (2016), os usuários possuem os seguintes direitos diante dos manipuladores de dados: de obter confirmação se seus dados estão sendo tratados ou não; quando da resposta positiva, ser informado sobre quais as finalidades, categorias de dados pessoais, destinatários ou categorias de destinatários dos dados ou mesmo terceiros e organizações internacionais; informar o prazo previsto a conservação dos dados e não sendo possível,quais os critérios para determinar o prazo de utilização.

Ademais, enaltece Ferrer (2021) quanto ao RGPD (2016), que o direito do usuário solicitar, ainda, a retificação ou supressão de dados; de limitar o tratamento relativo a suas

questões íntimas; o direito de apresentar reclamação à autoridade de controle; ou mesmo saber se há existência de decisões autônomas pelas máquinas a partir de seu perfil, torna o direito de conhecer como são utilizados os dados imensamente significante, pois permite a partir desse regulamento ter acesso a informações significativas e lógicas, cujo desrespeito pelos responsáveis no tratamento de dados, são sancionados pela própria lei.

Estas possibilidades normativas, entretanto, ainda não são a realidade do Brasil, possuindo carências enormes do ponto de vista legislativo, sendo necessário precisa avançar nessa construção regulatória de inteligência artificial, para melhor proteger a sociedade diante do uso abusivo desta por empresas dos mais diversos seguimentos ou nos moldes do controle social abusivo realizado por entes estatais, tornado preocupante tal letargia brasileira.

b) Risco de Irresponsabilidade de Máquina

Segundo Caitilin Mulholland (2020, p.328) as máquinas com inteligência artificial pautadas em algorítimos, são capazes de aprender de modo independente, passando a tomar decisões que muitas vezes não possuem a intervenção do ser humano, ou seja, a máquina a partir da análise de dados toma decisões gerando iniciativas que podem em alguns casos, serem diferentes dos objetivos dos entes empresariais dos objetivos dos entes empresariais responsáveis e, portanto, com potencial de causar enormes e irreparáveis danos.

A tomada de decisão autônoma por parte de uma máquina, através do aprendizado de máquinas (*machine learning*), pode se processar pela captação de imagens, sons, desenvolvimento sensorial, reconhecimento de padrões a partir da programação e imitação da tarefa cerebral, processando e gerando inferências equivalentes às dos seres humanos (MULHOLLAND, 2020, p. 331); através de métodos analíticos que lhes permitem aprender e tomar decisões, porém, apesar desta capacidade, nem sempre a tarefa é bem executada.

Esta autonomia realizada empregada pela máquina torna-se altamente perigosa na gestão da segurança das pessoas, uma vez que a utilização de robôs (por exemplo) pode culminar no processo decisório automático (MULHOLLAND, 2020); substituindo a autonomia decisória do ser humano (com seus valores, sentimentos, moral, regramento jurídico e limitações), pela decisão autônoma cujos resultados, por vezes, são imprevisíveis.

Assim, há questionamentos relacionados à irresponsabilidade civil do ente empresarial, e também sobre a irresponsabilidade quanto à máquina, pois ao se retroalimentar de dados e agir de modo autônomo, pratica atos diferentes dos objetivos para o qual foi criada pelo proprietário ou engenheiro.

Tal excepcionalidade e novidade para o Direito precisa ser reavaliada pelo legislador, haja vista, ser uma situação até o momento, atípica do ponto de vista jurídico, vez que a maquina não é um ente com personalidade para ser responsabilizada em primeiro plano, tornando-se uma ocorrência *sui generis* a partir do processamento do algoritmo da máquina com base no ao acúmulo de informações e retroalimentação do aprendizado.

Para além da responsabilização, há também a questão da ruptura do consentimento como direito básico do usuário, que fica relegado a segundo plano no trabalho autônomo da máquina, violação que também comporta maiores discussões.

Na mesma seara comparativa, nos revela Ferrer (2019, p.276), da análise da Lei Orgânica de Proteção de Dados Pessoais e garantia de direitos digitais da Espanha[41], mesmo em situações de doença e tratamento da saúde, há a necessidade de *consentimento* por parte do paciente na discussão sobre uso dos dados e informações pessoais, devendo inclusive, ser realizado por escrito, haja vista, a importância da consciência e liberdade individual.

Assim, na Espanha, mesmo tendo em risco a integridade física diante de uma assistência a saúde, é importante que cada pessoa individualmente considere agressivo ou não seu tratamento, estimando ou desestimando se é facultativo ou não, determinada intervenção médica, tendo a perspectiva da liberdade como pressuposto fundamental (FERRER, 2019); logo, em situações que não colocam em risco o bem maior universal que é a vida, o consentimento não pode ser relegado, sob qualquer hipótese, diante de novas tecnologias.

c) Risco de Irresponsabilidade Penal

Do ponto de vista penal, a Lei Geral de Proteção de Dados (2018) possui enorme lacuna e não pode ser aplicada de modo amplo no âmbito penal, nem da segurança pública pois há limitação expressa em seu texto (art.4º), fato que a limita diante dos incidentes cibernéticos ligados à cibercriminalidade ou no escopo da política criminal, diferentemente do RGPD (2016) da Europa, na qual se inspirou.

Assim, para os fins de segurança pública; defesa nacional; segurança do Estado; repressão das infrações penais, tal normativa possui vácuo legislativo perigoso, demonstrando incapacidade para responsabilização penal, notadamente levando a necessidade dessa correção para o âmbito da responsabilização penal.

[41] ESPANHA. *Ley Orgánica de Protección de Datos Personales y garantía de derechos digitale*. 05 Dec. 2018.

Apesar da LGPD (2018) se apresentar como evolução legislativa e objeto de defesa do usuário da internet, apresentando dez princípios relativos ao tratamento de dados pessoais: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas; o arcabouço jurídico mais robusto e preparado para a devassa de dados é necessária e urgente.

Nessa direção, para fins de consideração sobre a importância da aprovação de uma LGPD- Penal, é importante conceber segundo relatório de 2020 da Axur (empresa de segurança cibernética), que houve um amento de 99,2% nos casos de incidentes ligados ao *phishing* (páginas falsas) em relação aos dados de 2019; e de todas as invasões identificadas nesta modalidade, 41,1% desses *phishings* foram do setor de comercio digital (*e-commerce),* no total de19.784 casos. (AXUR, 2020; 2021)

No que tange ao vazamento de dados dos cartões de crédito 98,93% dos cartões de créditos expostos na internet, estavam dentro da data de validade no momento da detecção. Em 2021, houve redução dos crimes monitorados, contudo, ainda causando grande impacto econômico nos usuários. (AXUR, 2020; 2021)

4.2.2 Risco na potencialização dos crimes cibernéticos

As técnicas de inteligência artificial potencializam e ampliam a ocorrência das fraudes do âmbito penal, quanto do âmbito da irregularidade civil no trato de dados, em especial, com o uso de robôs para captação de dados e criação de perfis de consumo e utilização das redes sociais.

O aumento dos crimes cibernéticos passaram a ter consequências devastadoras para pessoas e empresas tanto no que tange ao vazamento de dados sensíveis da população, quanto relativos aos dados de diversas organizações sensíveis (algumas, inclusive, vulnerabilização serviços essências no país afetado)[42], além do impacto econômico e da violação de direitos fundamentais que esta realidade tem representado.

---

[42] Os Casos "JBS" paralisou a produção de alimentos e o "*Colonial Pipeline - EUA*" paralisou a produção de combustíveis e da Irlanda e Suécia e são exemplos de ciberataques que comprometem a infraestrutura crítica de um país em razão da essencialidade do produto que estas produzem. No caso da JBS, empresa brasileira que é a maior processadora de carnes do mundo, esta teve sua fábrica nos EUA atacada em 30 Mai 2021, paralisando a cadeia de alimentos, produção e distribuição, por uma semana para a América do Norte e Austrália. No caso "*Colonial Pipeline*" houve severa afetação na produção de petróleo dos EUA, paralisando a oferta de gás e outros produtos em toda a região oeste do país, acredita-se que a companhia pagou um resgate de US$ 4,4 milhões ao grupo criminoso. Disponível em https://www.securityreport.com. br/destaques/ransomware-segue-gerando-caos-na-industria-e-jbs-se-pronuncia-sobreciberataque/#.YZ2PGFXMLIX; e em http://Jbsfoodsgroup .com/articles/jbs-usa-cyberattack-media-statement-may-31. Acesso em 20 Fev. 2022.

Merecem destaque nessa ameaça os casos ocorridos com os negócios empresarias da “JBS” empresa brasileira considerada a maior processadora de carnes do mundo e que sofreu um ataque *hacker* em 30 Mai 2021, paralisando toda a cadeia produtiva de alimentos da sua unidade nos Estados Unidos da América, inclusive afetando a distribuição por uma semana, para a América do Norte e Austrália. (JBS; SECURITY REPORT, 2022)

No caso da *Colonial Pipeline,* ocorrido nos EUA, houve severa afetação na produção de petróleo, paralisando a oferta de gás e seus derivados em toda região oeste do país e em razão do crime a companhia pagou resgate de US$ 4,4 milhões ao grupo criminoso.

Todos esses ataques ou incidentes cibernéticos comprometeram a infraestruturas críticas de sistemas informáticos desses países, com grave prejuízo a sociedade, em razão da essencialidade dos produtos e serviços que estas fornecem, portanto, demonstrando que tais crimes podem ter consequências de grande porte.

Com estudos em Portugal, Daniela Santos, investigadora do Centro Nacional de Cibersegurança, relata que houve uma tendência de aumento em número e sofisticação dos ciberataques em relação a anos anteriores, fruto da necessidade do distanciamento entre as pessoas e do incremento das atividades laborais que passaram a ser realizadas por milhões de pessoas, em poucos dias, pelo método do teletrabalho. (SANTOS (2020)

Nessa direção, reforça como visto anteriormente, que o fenômeno da Covid-19, teve o condão de modificar diversos processos na sociedade e com forte transformação no âmbito do trabalho, que sofreu um revés a partir da necessidade dos usuários de se conectarem por meio virtual. (SANTOS, 2020)

Como retrata, houve forte impacto, inclusive, nas atividades ligadas a espionagem visando o roubo de informações sensíveis das pessoas e da propriedade intelectual das organizações, fato também identificado. Daniela Santos (SANTOS, 2020; p.4)

Tal realidade deixa claro, a concepção de que este fenômeno de aumento da cibercriminalidade não ocorreu apenas no Brasil, mas também, em Portugal e na maioria dos países do mundo, de modo simultâneo e com caráter global, trazendo a importância da cooperação internacional que a discussão da temática.

Nessa linha, a agência do *Federal Bureau Investisgation* (FBI, 2022), que faz um controle fino dos crimes cibernéticos mais exponenciais na América do Norte, monitorando também o que ocorre no mundo, expôs que os principais golpes registrados por aquela agência de investigação foram os ligados ao acesso aos dados sensíveis e das organizações.

O FBI apresentou como principal crime cibernético ocorrido durante a pandemia o comprometimento do email comercial de diversas instituições, em seguida apresentou como

segundo mais recorrente o roubo de identidade e informações pessoais, com dados ligados ao número de seguro social das pessoas. (FBI, 2022)

Seguiram-se, como terceiro na ordem de ocorrência, a implementação de "*ransomware",* programa malicioso que impede de acessar os arquivos pelo proprietário, no qual os cibercriminosos exigem pagamento para devolver o acesso a tais dados digitais (sequestro de dados), atingindo pessoas e também diversas empresas, afetando de sobremodo as informações o sigilo industrial.

Na sequencia, a realização dos *"spoofing"* e *"phishing"*, espécie de esquemas que induzem o usuário a determinada página falsa (*links*) e os induzem a fornecer dados sensíveis, apresentando ainda, o advento dos predadores virtuais *(predatores on line)* que são ameaças voltadas a cooptação e vitimização de crianças e adolescentes, ocasionando quebra da privacidade e segurança destes. (FBI, 2022)

Na mesma direção, o Grupo de Resposta a Incidentes de Segurança na Internet[43] (CERT.br, 2021), órgão governamental que monitora os incidentes cibernéticos no Brasil, registrou em 2019, o total de *"301.308 notificações [...], número que foi considerado o maior da série histórica, sendo 90% maior que o número de notificações recebidas em 2018";* enquanto que em 2020, as notificações ficaram na ordem de 665.079, redução de 24%.

A eclosão das notificações no ano de 2020, coincidiu, com a modificação brutal do uso da internet por motivo da pandemia, boa parte para o trabalho remoto, entretenimento e relações de consumo, além da perspectiva ligada engenharia social, modo natural de desproteção realizada pelo usuário da internet.

Tal redução, entretanto, também pode levar a presumir o maior investimento estatal e da iniciativa privada para a prevenção de cibercrimes, em especial, nos eventos ligados aos links do governo federal para assistência social e para proteção do trabalho remoto, além das campanhas de informação à população.

Não obstante, essa redução nas notificações em geral relatada pelo Grupo de Respostas a incidentes, não eximem a tentativa dos ataques ocorridos a servidores web, que aumentaram em 19% em relação a 2019. (CERT. br, 2021)

Em números absolutos o total de 26.567 casos em 2020, e os ataques de força bruta contra sistemas de gerenciamento de conteúdos que tiveram por objetivo adquirir senhas das

[43] CERT.br – é o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil é mantido pelo NIC.br, do Comitê Gestor da Internet no Brasil, e atende a qualquer rede brasileira conectada à Internet. https://www.cert.br/.

contas de administração dos sistemas, com vistas acessar todos os dados sensíveis contidos no sistema informático do usuário.

Por conseguinte, no que se refere às máquinas comprometidas por invasão cibernética, houve um aumento de 130% maior que em 2019 (CERT. br, 2021), fato é que os instrumentos de inteligência artificial, ampliam e potencializam tal criminalidade cibernética, reforçando a necessidade da prevenção deste risco.

4.2.3 Risco de Desequilíbrio da Ordem Econômica

Há riscos significativos no âmbito econômico além do impacto no âmbito da privacidade e da proteção dos dados e da própria vida, sendo os crimes cibernéticos capazes de afetar também a ordem econômica do país, além dos dados dos clientes.

A afetação das organizações públicas, organizações e empresas privadas com seus segredos industriais além de dados operacionais imprescindíveis, levam a um impacto enorme que podem se estender a usuários comuns, a partir do acesso ilegal e criminoso aos dados, bem como, às relações ligadas às estruturas financeiras e econômicas do país.

Exemplos de impactos financeiros foram os realizados por meio de falsificações de grandes marcas globais, que gerou do ponto de vista comercial, impacto social a partir do não recolhimento de impostos e mitigação de receitas de empresas consideradas líderes de mercado e internacionalmente conhecidas.

Em razão da utilização do ambiente remoto e do advento das compras *on line*, que dependeram tais negociações comerciais em razão do distanciamento físico da população, a falsificação de páginas e ofertas de produtos falsos geraram impacto econômico ao país.

O fenômeno da pandêmica que levou a superconectividade das relações comerciais na internet, unida à mitigada capacidade de fiscalização estatal ou privada sobre o intenso ambiente negocial, permitiram um ambiente favorável aos abusos, fraudes e crimes cibernéticos de toda a sorte.

Tem-se nessa realidade que "*ferramentas de colaboração, como Google, Dropbox e Microsoft, ou marcas de compras online como Amazon e PayPal, ficaram entre as 10 principais marcas falsificadas em 2020*". (IBM, 2021)

Relevante também, foi o caso da Adidas cuja venda de seus tênis *Yeezy* e *Superstar* (lançamento de grande desejo da juventude em 2019), teve um prejuízo no valor de US$ 1,3 bilhão (dólares) em razão da venda de produtos falsos pela internet, cujo impacto econômico demonstrou-se enorme mesmo para uma empresa como a Adidas. (IBM, 2021)

Na condicionante de vulnerabilidade dos dados sensíveis por meio das empresas, a pesquisa com 5.600 negócios de porte médio da Europa, Américas, Ásia-Pacífico e Ásia Central, Oriente Médio e África, intitulada *The State of Ransomware 2022*[44], revelou-se que a maioria já sofreram ataques cibernéticos. (SOPHOS, 2022)

Destas, 11% informaram ter pago resgate de US$ 1 milhão ou mais para hackers no ano de 2021, superior aos 4% relativos de 2020, ademais, quase a metade das empresas (46%), sofreram esta extorsão e tiveram dados criptografados e pagaram efetivamente para ter de volta as informações. Não obstante, muitas empresas que já tinham sido atacadas em 2020, mesmo conhecendo a necessidade de backups de dados, mais de 26% foram atacadas novamente e voltaram a pagar resgate, ou seja, permaneceram sem ações preventivas quanto a ação criminosa cibernética. (SOPHOS, 2022)

Quanto ao tempo médio de recuperação de danos e suspensão de atividades girou em trono de um mês, sendo que em 90% dos casos houve afetação da capacidade operacional do negócio, registrando ainda, em 86% das empresas, perda de receita em razão dos ataques cibernéticos, com fortes impactos econômicos para além dos danos diversos inerentes. (SOPHOS, 2022)

O relatório da Sophos (2022) expôs ainda, que para se recuperar de um ataque cibernético desta natureza, ligado ao *ransomware*, o custo médio empresarial em 2021, foi da ordem de US$ 1,4 milhão (de dólares), como pode ser visualizado no quadro abaixo.

É possível observar que na evolução de 2020 para 2021, algumas nações passaram a reduzir os ataques cibernéticos criando estratégias de segurança consideráveis, como demonstra o relatório relativo a Áustria (-90%), Canadá (-66%), México (-57%), Noruega (-64%), Suécia (-46%), Inglaterra - UK (-45%), Estados Unidos (-49%) e Brasil (-16%), que apresentou tímida redução anual. (SOPHOS, 2022, p.18)

Outros países tiveram um acréscimo considerável de vulnerabilidades e ataques de *ransomware*, o que revela a necessidade de aumentar a maturidade cibernética de tais nações para aprender a prevenir tais ataques, nessa dinâmica.

Nesse contexto, a República Tcheca com aumento relevante na ordem 589%, Nigéria com aumento nos ataques na ordem de 644%, Arábia Saudita com registro de mais 212%, Israel com mais 148%, Emirados árabes Unidos (UAE) com crescimento de ataques em 144% e Chile com 116% a mais que 2020, conforme relatório da Sophos (2022).

[44] Estado do Ransomware 2022.

Na mesma direção do que já havia sido retratado em relatório da McAfee (2020, p.13)[45], em parceria com o Centro de Estudos Estratégicos Internacionais (CSIS), estima-se que os custos estão sendo cada vez maiores de boa parte da classe empresarial.

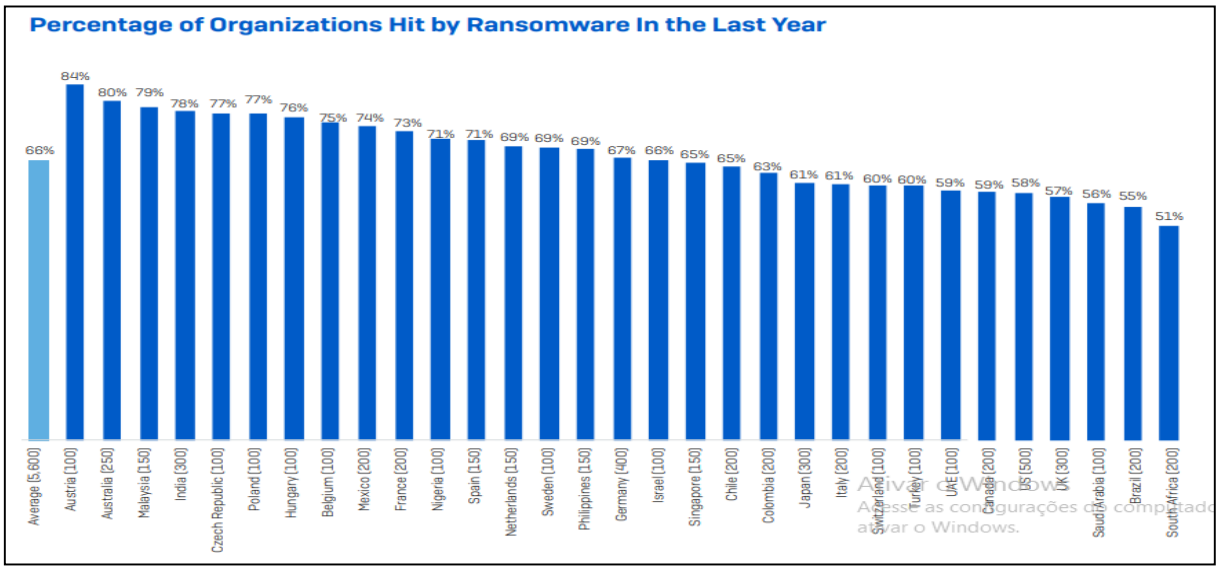
Em 2020, os custos com cibercrimes já haviam ultrapassado os trilhões de dólares, prejuízos que levaram a gastos na ordem de US $ 945 bilhões (de dólares), somados a U$ 145 bilhões (de dólares) com prevenção e segurança da informação. (MCAFEE, 2020; p.13)

Atualizando os dados para 2021, conforme relatório da Axur (2022) os prejuízos com fraudes virtuais, alcançaram a absurda marca de U$ 6 trilhões (de dólares) no mundo, registrando o equivalente a quatro vezes o Produto Interno Bruto (PIB) do Brasil de 2020.

Relata a Axur que as previsões sobre cibercrimes no futuro, girarão em torno de U$ 10,5 trilhões (de dólares) em prejuízos até 2025; reforçando que tais custos teve aumento considerável, com ataques cibernéticos que permeiam a exigência de pagamento de dinheiro para reaver os dados *sequestrados* da empresa e dos clientes, modalidade digital de extorsão, ampliada significativamente entre 2020 e 2021. (AXUR, 2022)

Como expôs a Sophos (2022), 66% das empresas em média, sofreram ataques de *ransomware* em 2021, nesta modalidade de extorsão com exigência de pagamento para devolução dos dados, demonstrando um aumento de 37%, em relação ao ano de 2020.

GRÁFICO 2
PORCENTAGEM DE ORGANIZAÇÕES ATINGIDAS POR RANSOMWARE – 2021



[45] MCAFEE. *The Hidden Costs of Cybercrime*.(Tradução livre: Os custos ocultos do crime cibernético). 07 December 2020. Disponível em https://www.mcafee.com/enterprise/pt-br/about/newsroom.html acesso em 15/12/2020.

Fonte: Sophos (2022, p.12)

No estudo, o Brasil aparece com 200 empresas pesquisadas, tendo havido entre estas 55% de empresas atingidas por ataques cibernéticos do tipo r*ansomware*, que sequestra dados, enquanto que a nação mais atingidas por ataques foi a Áustria, tendo registrado 84% das 100 empresas pesquisadas, como afetadas por crimes cibernéticos.

Do ponto de vista da prevenção 94% das empresas realizaram seguro cibernético e afirmaram ter realizado mudanças no alcance das apólices no último ano, para contemplar políticas mais complexas e caras de cobertura; não obstante, a quantidade de empresas seguradas foi inversamente proporcional as que compram os produtos, tendo havido redução no mesmo período.

A influencia negativa que essas fraudes ocasionam no âmbito econômico e diante da inteligência artificial que amplia o risco dessa criminalidade, em razão da automação de estratégias criminosas que a tecnologia permite; terminam por favorecer o desequilíbrio das relações comerciais e impactam economicamente no direito, vez que, por consequência, ampliam processos de desigualdade social e afetam a população mais carente, pela perda de reserva e receitas econômicas destas nações.

Notadamente os recursos utilizados como páginas falsas, manipulação de grande quantidade de dados, cruzamento de banco de dados com informações privilegiadas, utilização de robôs na captação de informações sensíveis, são de grande relevância na expansão de tal modalidade criminosa cibernética, tornando-se enorme desafio ao mundo do direito gerar instrumentos para sua mitigação.

4.2.4 Risco na dependência da cibersegurança privada

A dependência dos sistemas de cibersegurança dos entes privados, torna-se problemático a partir da insegurança que existe nos programas de conformidade (*compliance)* de tais empresas (quando existem) e, do nível de ética implementado por tais atores privados. Ademais, não parece ser a melhor solução diante do caráter capitalista e dos fins lucrativos que buscam tais organizações.

Deste modo, parece forçoso que o ente estatal adentre em determinado momento visando regular e promovendo tal segurança de caráter pública e gratuita, inclusive, para que tenha efetivo alcance geral visto que essa premissa fica prejudicada com recursos de segurança

cibernética privada, vez que pessoas hipossuficientes não podem pagar pelos custos desses serviços que demandam grande investimento em razão das pesquisas que esta empresas realizam.

Considerando que os organismos públicos também devem estar comprometidos com o Estado Democrático de direito, e com o patrocínio da proteção dos bens relevantes da sociedade, deve proteger a incolumidade das pessoas ofertando o direito fundamental à segurança pública, com as respectivas limitações, que permitam coadunar e equilibrar o direito a privacidade.

Logo, permitir o exercício das liberdades inerentes à intimidade, privacidade e autonomia da vontade no uso de informações pessoais sensíveis, juntamente com o direito a segurança cibernética, é algo que deve ocorrer ainda que hajam críticas dos que acreditam que o Estado não deve estar presente para regular a vida em sociedade, posto que a vulnerabilidade da manipulação privada dos dados sensíveis é também perigosa e igualmente preocupante.

Grande exemplo deste risco no uso da inteligência artificial, foi o corrido recentemente, em razão da guerra iniciada pela Rússia em fevereiro de 2022 contra a fronteiriça Ucrânia, que teve seu território invadido pelo exército sob ordem do presidente *Vladmir Putin*, tendo por reação diversas medidas restritivas e sanções administrativas e comerciais contra pessoas e empresas da agressora, por países europeus e Estados Unidos.

O risco ao ambiente da tecnologia da informação, foi acentuado com o alerta emitido na Seção 7 da Lei do (BSI) [46], Escritório Federal de Segurança da Informação da Alemanha, advertindo contra o uso de software de proteção contra vírus e serviços em nuvens do fabricante russo de segurança cibernética, *Kaspersky*[47], sugerindo potenciais riscos para a segurança de tecnologia em razão destes serviços possuírem amplas autorizações de sistema que podem colocar a autoproteção em risco. (BSI, 2022)

O alerta sugeriu que os sistemas poderiam ser utilizados pelo fabricante para espionagem ou ataques cibernéticos, tendo recomendado substituição por produtos similares de outras empresas, desde que possuíssem conexão criptografada baseada em confiabilidade.

Não obstante, a empresa emitiu nota informando que tal alerta foi mera especulação e sem fundamento técnico, que nos vinte e cinco anos que atua nunca houve evidência de abuso

[46] BSI - *Bundesamt für Sicherheit in der Informationstechnik* refere-se ao Escritório Federal de Segurança da Informação;

[47] Os dados estatísticos coletados com a empresa para os fins deste trabalho foram precursores a guerra entre a Rússia e a Ucrânia, sendo considerados de referência de qualidade no âmbito dos dados de segurança cibernética, portanto, as informações anteriormente coletadas permanecerão expostas nesta pesquisa.

ou que tenha atuado para fins maliciosos e informou que deixará de apresentar aos principais fabricante de equipamentos industriais daquele país, informações da "*Kaspersky ICS-CERT sobre vulnerabilidades críticas em* seu *software* e *hardware, uma organização aclamada por esses mesmos fabricantes e pelo seu trabalho de divulgação".* (KASPERSKY, 2022)

Por tudo, a reflexão que se realiza é a de que qualquer empresa de segurança cibernética contratada por usuários em todo o mundo, podem monitorar e ter acesso pleno as informações de empresas e pessoas, manipulando-as com instrumentos de *big data*, que a depender do contexto político pode ser utilizado como uma ferramenta de vantagem competitiva de poder.

Desta forma, tais informações podem servir a qualquer tempo tanto para o ambiente empresarial, mas também, serem direcionadas para questões de ordem política, de governos sob o viés autoritário ou não, podendo ser instrumento utilizado sob outro olhar que não os vinculados aos valores democráticos desta sociedade.

As possíveis pressões sobre tais organizações empresariais que porventura possam ocorrer sobre a manipulação de dados da população de outros países, dependerão, em ultima racionalidade, dos próprios instrumentos internos empresariais de *compliance* que a organização possui, com maior ou menor nível de imparcialidade, a depender do contexto político e econômico de cada nação.

4.2.5 Risco na manipulação de grande quantidade de dados (*big data)*

A modificação na capacidade de processar dados pelas máquinas físicas e por programas de computadores e o desenvolvimento das tecnologias de processamento em nuvem (*cloud computing*), além da expansão e manipulação de grande quantidade de dados *(big data)* na rede de protocolos da internet.

Tais tecnologias favorecidas pelo desenvolvimento e aplicação dos estudos sobre algorítimos matemáticos, robótica e inteligência artificial está permitindo o uso pelas entidades das esferas públicas e privadas.

Os estudos do pós-guerra no século XX, definiram duas principais linhas de implementação da IA, a primeira com base na engenharia do conhecimento que permitiu a *informatização da sociedade* impulsionada pela democratização do acesso às novas tecnologias; não obstante, as exclusões retratadas por Castells (2013) na análise da sociedade em rede, tendo por consequência o fato de que 65% da população mundial atualmente, utilizam a internet e alimentam essa engenharia com dados pessoais. (FGV, 2021)

Na segunda linha, observa-se o *conexionismo*[48], que permitiu a interconexão e conectividade entre tecnologias de gerações e modelos diferentes, expandindo o uso da internet e tornando o ciberespaço um local de realização e resolução das mais diversas tarefas; tais instrumentos favoreceram maior controle social, mas também permitem, se constituir meios de manipulação de dados sensíveis da população para uso irregular de entes públicos e privados, fragilizando e vulnerabilizando a segurança das pessoas comuns. (FGV, 2021)

O Estado em rede passou também a utilizar tais recursos para promover o controle social e prevenir criminalidade em diversos países do mundo, com olhar especial para os Estados Unidos da América, China, Rússia, Europa e mais recentemente no Brasil, a apartir da estratégia governamental de digitalização do país e as iniciativas para segurança cibernética[49] para combate à criminalidade em expansão, mas também, sob o viés do forte controle social.

Do ponto de vista técnico a quantidade de dados ao decorrer do tempo, quando analisados mediante técnicas de estimativas matemáticas produzem um valor tal que por meio de algorítimos fundamentam a atuação das máquinas tecnológicas cujo processamento de informações leva ao desenvolvimento de tarefas, através de similitudes e aproximações analógicas de dados comuns. (PROVOST e FAWCETT, 2013)

Há nessa concepção, um trabalho de *predição* ou antecipação de possibilidades futuras que podem ocorrer, *mas que de fato nunca se sabe se efetivamente acontecerá efetivamente*, a apartir de métodos probabilísticos que são utilizados para prever a ocorrência de determinados comportamentos sociais, tal técnica aplicada às máquinas computacionais e o uso de uma enorme quantidade de dados, automatizam essa predição para o ente estatal.

Nesse sentido as máquinas computacionais passam a realizar o controle e a vigilância, determinando grupos que devem possuir maior atenção dos entes estatais por demonstrarem maior risco social.

Tal instrumento torna-se então deveras preocupante no âmbito da segurança pública e no uso desses recursos como instrumento de política criminal, pois a utilização de recursos probabilísticos com base em algorítmos matemáticos probabilísticos, por vezes, desembocam em contextos discriminatórios, a partir dos dados históricos que alimentaram o bancos de dados, gerando graves distorções inerentes a prevenção social.

---

[48] XAVIER (2020).

[49] A Estratégia Nacional de Segurança Cibernética (E-Ciber) promove governança no âmbito da segurança da informação pelo governo federal, conforme Decreto nº 9.637 de 26/12/2018.

Há que se reconhecer que o Brasil diante do contexto histórico escravagista e excludente das populações negras possui uma enorme quantidade de processos penais condenatórios e de encarceramento que penalizam em maioria a jovens, do sexo masculino, negros e pobres do país e do ponto de vista histórico esse banco de dados estaria excessivamente contaminado com a *cultura de exclusão* da população negra.

Logo, do ponto de vista algorítmico, tal historicidade pode ser nefasta no âmbito da política criminal, vez que o banco de dados utilizados pelas tecnologias da inteligência artificial para *predição* de futuros crimes e perfis de supostos criminosos, tendem a recair modo discriminatório sobre a população negra, como destinatária do trabalho preditivo de controle social com foco nas sanções criminais.

Outro aspecto importante nessa análise é a distorção sofrida no emprego da tecnologia de *big data* para o âmbito diferente para o qual foi criado, conquanto, a manipulação de quantidade de dados pautada em inteligência artificial, se desenvolveu para automação industrial e na produção, no escopo da indústria 4.0. (SCHWAB, 2019)

Entretanto, o fenômeno de digitalização da sociedade, levou a inovação da *big data* para as máquinas em geral, tornando-as mais autônomas e unidas a outras técnicas de inteligência artificial como algorítmos, vídeomonitoramento, robótica e reconhecimento facial, pode ser empregada no monitoramento social, *da segurança pública*, migrando inclusive, para a dimensão da *segurança privada*, apresentando novos contornos e desafios.

Note que o processo de acumulação de informações por meio de base de dados diversas através da internet e do monitoramento de informações, o trato por entes públicos e privados,tornou-se questionável na efetivação das técnicas para o controle da sociedade, dada o potencial de impactar na dignidade da pessoa humana, a partir da manipulação dos dados sensíveis, sem regramentos adequados ainda, no Brasil.

Busca-se nesta pesquisa levar o leitor a reflexão sobre a técnica de *big data*, sobre a necessidade de responsabilização do agentes da implementação e monitoramento da IA e da imprescindibilidade de neutralidade dos dados inseridos no banco de dados do sistema, haja vista, a sensibilidade dos dados a serem protegidos, ademais, contrapondo-se expressamente a cultura de ganho econômico a todo custo, que deixe de lado questões relativas a igualdade racial a partir da seletividade dos sistemas, que de modo discriminatório, pode afetar grupos vulneráveis historicamente subjugados socialmente.

Tais preocupações conduzem a análise da legitimidade e validade no processamento de tais dados sensíveis, de modo automático por computadores incrementados

com inteligência artificial e algorítimos capazes de promover o cruzamento de informações, sem a autonomia decisória de seus usuários, discussão que precisa ser ampliada.

Essas informações constituem-se fenômenos probabilísticos sobre pessoas, lugares, tarefas e probabilidade para o crime, realidades probabilísticas de riscos, que nem sempre poderá de fato ocorrer, mas que a máquina considera como verdadeiro e expõe como risco criminológico, especialmente, quando permeados com algorítmos discriminatórios.

A tecnologia de inteligência artificial tem a potencialidade de gerar uma expectativa preocupante, a partir do cruzamento de dados com algorítimos matemáticos, com grande capacidade de tratamento de dados de modo irregular ou até ilegal, assim tem o condão de instaurar uma nova faceta no âmbito do controle.

O cruzamento de informações diversas possibilita interagir com outros riscos aqui delineados, a partir da formação robótica de perfis e da capacidade de monitoramento do comportamento e dados das pessoas, e a depender de como são empregadas tais informações, podem ocasionar preocupantes violações às liberdades, diretamente interligadas a afetação da dignidade humana, tais concepções e estudos precisam ir além do escopo deste trabalho.

4.2.6 Risco das informações sob custódia de entes públicos

A atuação do Estado como ente protetor da sociedade é algo importante a se conceber quando existe um bom desenho de segurança cibernética que permitem limites para o controle e vigilância social, ao mesmo tempo, em que possibilita a tutela da segurança digital das pessoas de modo preventivo.

Há, contudo, uma preocupação e um risco iminente que vem se concretizando cada vez com mais frequência, que é o vazamento de dados das informações dos bancos de dados públicos, bem como, a manipulação política de informações sensíveis.

Não obstante, a representação social de que os banco de dados do governo seriam mais confiáveis, foram relativizados após diversos incidentes, reiterados, que tem demonstrado enorme fragilidade de tais sistemas para a concentração de dados da população, em especial, das informações mantidas em nuvem, que se tornam objeto de interesse dos criminosos cibernéticos, em razão de concentrar grande nível de informações.

A inovação trazida pela Lei nº 14.129 de 29 de março de 2021, dispôs sobre princípios, regras e instrumentos para realização da plataforma do *Governo Digital* e para o aumento da eficiência pública, trazendo muitos pontos positivos.

Estabeleceu como diretrizes principais: a desburocratização e modernização da relação do poder público com a sociedade, mediante serviços digitais; a disponibilização em plataforma única do acesso às informações e aos serviços públicos; a possibilidade aos cidadãos e às pessoas jurídicas de demandar serviços públicos por meio digital, sem solicitação presencial. (BRASIL, 2021)

Alega também, promover a transparência na execução dos serviços públicos e o monitoramento da qualidade desses, não obstante, centralizou a atuação dos serviços estaduais em uma plataforma única que interage com um banco de dados nacional, o domínio *gov.br* ligado ao Ministério da Economia. (BRASIL, 2021)

Não obstante, os vazamentos de dados tem sido constantes em diversos órgãos estatais e em todas as instâncias de gestão[50], a exemplo, da plataforma do Sistema Único de Saúde (SUS) ter ficado fora do ar em meio a pandemia; estes fatos tornam preocupantes os riscos relativos a guarda de informações consideradas sensíveis dos cidadãos, inclusive, no âmbito da saúde que estão sob custódia dos sistemas públicos, além da quantidade de informações sensíveis acumuladas e a qualidade dessas para organizações criminosas.

Para se ter dimensão, segundo a Axur no relatório de atividades criminosas *on line* do Brasil em 2021, expõe que mais de 2,8 bilhões de dados sensíveis da população foram vazados e tornaram-se públicos, sendo que destes, mais de 43,3 milhões estavam relacionados a domínios de empresas, mas, 227 mil domínios eram pertencentes ao governo brasileiro; foram monitorados "*24 megavazamentos de dados"* no país**,** além dos vazamentos menores no ano de 2021. (AXUR, 2022)

Apenas em junho de 2021, os dados expostos corresponderam a 41,2% do total, demonstrando uma dinâmica diferente quanto a exposição de dados e manipulação pelos agentes mal-intencionados no âmbito nacional e no âmbito internacional, assim, havendo diferenças no *modus operandi* dos cibercriminosos a depender do local onde atuam.

Não obstante, há total interesse dos entes públicos no compartilhamento de dados para fins diversos, dois pontos de atenção atual são o *Decreto 10.046/2019*, que criou o banco de dados base do cidadão, para reunir informações existentes em diferentes órgãos da administração pública de modo compartilhado e o mais recente, o *Decreto nº 10.977/2022*, que regula a carteira digital, ambos acumularão informações em quantidade da população.

---

50 "*Suspeito de participação em ataque hacker ao Ministério da Saúde e outros órgãos do governo federal é preso na Bahia*." 19 out. 2022. Disponível em https://g1.globo.com/ba/bahia/noticia/2022/10/19/suspeito-de-participacao-em-ataque-hacker-ao-ministerio-da-saude-e-outros-orgaos-do-governo-federal-e-preso-na-bahia.Ghtml. Acesso em 20 out. 2022;

Note que no caso da carteira de identidade digital, apesar dos sistemas de segurança e código de verificação com barras bidimensional no padrão QR (*quick response code*)[51], estas serão utilizados dados com informações biométricas das pessoas.

Este Decreto expressa no art. 12, quanto ao cadastro biométrico: *"na expedição da Carteira de Identidade, será realizada a consulta biométrica no Serviço de Identificação do Cidadão"* (BRASIL, 2022), e no inciso VIII do mesmo artigo, a integração da carteira de identidade ao serviço de identificação será assessorada tecnicamente pela "*Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia".*

A realidade que se apresenta em verdade, é que o banco de dados do poder público concentra informações privilegiadas de boa parcela da população do Brasil e, tal concentração, torna-se um polo de interesse da cibercriminalidade, constituindo-se, uma custódia vulnerável às ações criminosas, ademais, aumentando o risco sobre informações sensíveis se dados biométricos forem alcançados por criminosos profissionais.

Para evitar abusos o Supremo Tribunal Federal (STF, 2022) decidiu nas ADI 6.649[52] e a ADPF 695[53], a restrição do compartilhamento de informações também aos entes do executivo governamental, criando mecanismos rigorosos de acesso ao *Cadastro Base do Cidadão, e* proibindo o compartilhamento de dados, senão, com requisitos, garantias e procedimentos da Lei Geral de Proteção de Dados (2018).

O STF também realizou prevenção quanto a atividade de *Inteligência Policial*, tendo restringido o acesso às informações sensíveis, a partir dos parâmetros fixados na ADI 6.529, determinando quando o ente precisar de acesso aos dados: a adoção de medidas proporcionais e estritamente necessárias ao atendimento do interesse público; instauração de procedimento administrativo com anterior e motivação; utilização de sistemas eletrônicos de segurança e de registro de acesso aos dados, visando responsabilização, e observância dos princípios gerais de proteção e dos direitos coadunando-se com a LGPD. (STF, 2022)

Tais decisões visam evitar a significativa e invasiva vigilância sobre as pessoas e se coaduna com o objetivo relacionado a *paz, justiça e instituições eficazes*, contidas no item 16 da agenda global da ONU 2030, de modo a não permitir que os dados sensíveis sejam usados de modo abusivo ou sob manipulação política pelos poderes, posto que o ente governamental deve atuar para tutelar direitos e não vulnerabilizando-os.

---

[51] Tradução livre: Código de Resposta Rápida.
[52] Disponível em https://portal.stf.jus.br/processos/verImpressao.asp?imprimir=true&incidente=6079238;
[53] Disponível em https://portal.stf.jus.br/processos/detalhe.asp?incidente=5938693.

4.2.7 Risco à propriedade intelectual, aos conhecimentos científico e tradicional

A propriedade intelectual que permeia a formação do conhecimento científico e tradicional diante da sociedade da inovação e do advento da quarta revolução industrial vem sendo brutalmente atingida, tornando-se elemento que merece atenção diante da construção e disseminação das formas de pensar, diante do advento da atual sociedade tecnológica.

Segundo Ramírez (2019), existe atualmente uma nova divisão internacional do trabalho que culmina com o desenvolvimento de uma economia baseada no saber e na sua difusão deste junto a sociedade; logo, a produção do conhecimento passa a ser aplicado como instrumento de desenvolvimento social mas também, atualmente como instrumento da propriedade intelectual.

Como expõe o Decreto-Lei nº 1.355, de 30 de dezembro de 1994, que incorpora no ordenamento jurídico brasileiro os resultados da rodada Uruguai de negociação comercial[54], em seu artigo 7º, a proteção dos direitos de propriedade intelectual deverá contribuir para a promoção da inovação e transferência e difusão da tecnologia para favorecer o bem-estar social, econômico e o equilíbrio dos direitos e obrigações, logo, sua afetação compromete, em última instância, o interesse público de modo amplo. (BRASIL, 1994)

Como retrata o pesquisador Manuel Becerra Ramírez a violação da propriedade intelectual, diante da evolução das revoluções tecnológicas, pode impactar além da economia toda a atividade humana, afetando de sobremodo o reconhecimento e a função das normas da propriedade intelectual. (RAMÍREZ, 2019)

Enquanto as tecnologias ampliaram o campo da inovação e possibilitou maior acesso ao conhecimento, inclusive, com redução de tempo e custos pela reprodução e distribuição da informação; contribuiu para a cópia indiscriminada e transmissão do conhecimento e da informação (com menos construção e reflexão), formando um sistema *capitalista cognitivo*, na concepção de Ramírez (2019).

Este sistema capitalista cognitivo, por sua vez, permitiu o marco jurídico da propriedade intelectual no primeiro momento, e enquanto segunda geração, a inserção desta PI no âmbito do comércio internacional, segundo Ramírez (2019); gerando para o autor das obras e produtos uma condição econômica e temporal, favorável a explorar os frutos de sua criação.

[54]A normativa foi acolhida no arcabouço do Tratado Internacional de Propriedade Intelectual administrado pela Organização Mundial da Propriedade Intelectual (OMPI), entidade internacional de direito público, situada em Genebra na Suíça e faz parte da ONU.

Não obstante, há uma preocupação considerável nesse contexto de formação do conhecimento, inicialmente relativo à desvalorização dos conhecimentos acumulados ao longo do tempo, diante da velocidade dos novos conhecimentos que surgem, substituindo com maior volatilidade a sabedoria anteriormente concebida.

Há um segundo prejuízo também evidente, que se estabelece quanto à fragilização dos conhecimentos científicos já construídos, e a exclusão dos conhecimentos tradicionais, sabedoria historicamente construída pela sociedade, diante desse capitalismo cognitivo que valoriza o conhecimento tecnológico.

Assim, a consequência prejudicial relaciona-se ao fato de que o sistema capitalista cognitivo, tem deixado de fora o conhecimento tradicional e a sua liberdade de expressão e exploração, nas diversas áreas do conhecimento como na medicina, música, poesia e outros, conforme a concepção ocidental do conhecimento. (RAMÍREZ, 2019; p.8)

No âmbito do conhecimento cientifico que antes se formava de modo livre e muitas vezes em momentos improváveis, o conhecimento passou a ser reduzido a uma forma mínima de construção, veloz e sem a racionalização do experimento e do tempo.

É importante conceber, nesse sentido, que o conhecimento tecnológico desse sistema capitalista cognitivo, cresce à custa das demais áreas do conhecimento, também, do conhecimento tradicional, cotidiano e do conhecimento científico (como os construídos pelos dos filósofos clássicos); ainda que em última instância, deságuem a novidade, no ato de patentear. (RAMÍREZ, 2019; p.8)

Fato é que as fronteiras entre a investigação tecnológica e cientifica estão se diluindo, formando o conhecimento científico-tecnológico despreocupado com a distribuição de riquezas e com a redução das injustiças sociais, e sim, com a formação de produtos tecnológicos, que possuem um valor no mercado e são protegidos pela propriedade intelectual renegando conhecimentos tradicionais de modo formal. (RAMÍREZ, 2019; p.16).

Segundo León Olive sobre os conhecimentos tradicionais e multiculturalismo, o pesquisador não se deve criar dicotomia entre sociedade do conhecimento e sociedade da inovação, assim, quando redes socioculturais funcionam como geradores de conhecimento, estas devem atingir objetivos voltados ao bem da sociedade. (OLIVE, 2014; p.15)

As condições adequadas, para Olive (2014), é que a formação do conhecimento na era da inovação possibilite a resolução de problemas específicos; portanto, devem se apropriar do conhecimento previamente existente (científico e tradicional) para compreender problemas atuais e propor soluções na dinâmica social emergente.

Ainda, na perspectiva de Olive (2014), a sociedade da inovação deve ser capaz de gerar conhecimento que não está disponível; que tenha em sua essência o intuito de proteger os conhecimentos tradicionais diante de apropriações indevidas e tenham estrutura não hierarquizada que permita o desenvolvimento livre de capacidades dos participantes para gerar conhecimento amplo às novas gerações, para converter conhecimento em ação.

Deste modo, a concepção de que tanto o conhecimento científico e o conhecimento tradicional possui a sua importância e não podem ser deixados de lado na formação cultural e intelectual da sociedade.

Sem dúvida, há fortes evidências de que os conhecimentos tecnológicos podem desempenhar um papel preponderante para o desenvolvimento da sociedade, porém, a reflexão de que todos os níveis de conhecimento devem estar presentes na formação das novas gerações, tem sua importância enquanto legado social relevante.

Tanto o conhecimento científico quanto o tradicional, ainda que permeados pelos conhecimentos tecnológicos, mais ou menos efêmeros ou voláteis, mesmo atrelados à velocidade digital, necessariamente, devem ser inseridos na formação das atuais e futuras gerações de mentes pensantes, pois as soluções da complexa relação humana social é dependente dos conteúdos dessa ampla formação que levem a criatividade para resolução dos desafios novos e velhos que se apresentam.

4.2.8 Risco para Liberdade Cognitiva do ser humano

a) Risco de violação das funções neurais e cerebrais *(Neurolaw)*

A utilização de Inteligência Artificial também apresenta risco à livre cognição humana, à mente das pessoas e à sua capacidade decisória a partir do aprendizado de máquina, quando adquiri a capacidade de distinguir como funciona o ato de pensar cerebral e como se forma o processo de decisão do indivíduo, podendo conceber a intervenção neural, para modificação da vontade do indivíduo ou mesmo tomar decisões sem consentimento.

Tal tecnologia tem como pano de fundo, os estudos sobre a *neurociência*, *neurotecnologia*, bem como, a n*anotecnologia,* técnicas unidas a inteligência artificial que estão sendo empregadas no escopo do melhoramento genético e na manipulação do cérebro humano, para construção de sistemas e funções cerebrais a partir de máquinas computacionais, com todos os riscos e benefícios que podem proporcionar.

Segundo Yuste & Bargmann (2017a) a sociedade está no tempo do *"NanoNeuro"* que comporta a união da nanotecnologia com a neurociência e tem por fundamento o emprego de *nanomateriais*, em escalas microscópicas no cérebro, visando registrar e estimular atividades neurais, podendo ser aplicadas em humanos sem a necessidade de modificações genéticas, sofrendo tal técnica, enorme apelo das Ciências Biomédicas, dado os benefícios para o tratamento de diversas doenças neurológicas.

Nesse sentido, como revela Yuste & Bargmann (2017a), estão em andamento diversos projetos ligados a *neurotecnologias* conjuntamente a *nanotecnologia* no mundo, sendo o projeto *US BRAIN* dos EUA, lançado em 2013, pelo governo Obama, e que tem como plano de trabalho para estudo dos circuitos e sistemas neurais em escalas de tempo e espaço em animais modelos e em humanos.

A União Europeia está desenvolvendo o projeto *Cérebro Humano (HBP*), que se esforça para a coleta e simulação de dados cerebrais em larga escala, tendo objetivos o desenvolvimento de infraestrutura científica para pesquisa do cérebro, neurociência cognitiva e experimentos de simulação cerebral, além da teoria da construção e *desenvolvimento de ciência computacional inspirada no cérebro*, projeto que funciona com sede na Suíça.

O Japão, por sua vez, lançou o projeto *Japan Brain/MINDS*, em 2014, com três objetivos iniciais: mapear a estrutura e funcionamento do cérebro e estudos genéticos; desenvolver inovação para manipular aspectos da atividade neural e constituir biomarcadores para distúrbios cerebrais. E a Coreia do Sul, anunciou projeto de mapeamento cerebral com foco em doenças cerebrais associadas ao envelhecimento, como foco no desenvolvimento de infraestruturar uma ciência do cérebro. (YUSTE & BARGMANN, 2017a)

Os estudos sobre *neurodireito* ou *neurolaw* se ambientam na direção dessa inovações neurotecnológicas e visa estabelecer garantias legais para que o *cérebro e a mente do ser humano não sejam manipulados cognitivamente* ou *hackeados*, pela IA.

O risco está justamente na promoção do aprendizado cerebral de máquina e esta possa afetar ou intervir na *decisão cerebral do ser humano*, assumindo a máquina, a identidade da pessoa, realizando o exame do que é correto ou incorreto, de modo autônoma. (BELLOSO, 2022)

As neurotecnologias têm o potencial real de alterar elementos da experiência psicológica humana em especial quando os recursos da neurociência são utilizados em consonância com a inteligência artificial, podendo expandir ou interromper sentidos de identidade dos indivíduos, comportando potencial impactante psicossocial.

A respeito da proteção da identidade humana, por exemplo, as neurotecnologias são capazes de modificar o funcionamento psicológico do indivíduo, podendo de modo positivo, tratar sintomas da depressão, transtorno obsessivo compulsivo, demência e estresse pós-traumático, contudo, gerando preocupação quanto à possibilidade de modificação da identidade pessoal. (GOERING; YUSTE, et. al., 2021)

O estado psicológico da pessoa é o responsável pela interpretação das experiências reais, porém, quando afetadas pelas alterações criadas pelos estímulos elétricos recebidos pelo cérebro, ou mesmo, da presença de dispositivos que fazem a leitura do cérebro para o controle das doenças, pode haver a alteração da identidade pessoal. (GOERING; YUSTE, et. al., 2021)

Nesse sentindo a neuroengenharia responsável precisa estar sendo acompanhada e sofrer a intervenção dos acadêmicos do direito, com a criação de dispositivos garantistas capazes de promover uma inovação responsável do ponto de vista dos dados sensíveis, em especial, das informações relativas ao funcionamento da estrutura cerebral.

A partir dessas concepções dos especialistas (YUSTE; GOERING; [et. al]; 2017b; p.161/162), delineiam-se cinco principais institutos do direito para proteger o cérebro humano da devassa da decisão cerebral de máquina:

-Direito à identidade pessoal;
-Direito à privacidade mental;
-Direito ao livre arbítrio decisório;
-Direito ao acesso equitativo das pessoas as melhorias cognitivas; e
-Direito à proteção contra a criação de vieses discriminatórios.

Tamanha é a preocupação e a realidade dessa ameaça por parte da inteligência artificial, podendo afetar a capacidade cognitiva do ser humano, que o Conselho da OCDE em 11 de Dezembro de 2019, adotou *Recomendação sobre Inovação responsável em Neurotecnologia,* tornando-se primeiro padrão nesse quesito e tendo o objetivo de orientar governos e antecipar desafios do ponto de vista legal, ético e social ocasionados pelas novas neurotecnologias, de modo a maximizar benefícios e minimizar riscos. (OCDE, 2019b)

Notadamente, é importante refletir que a tecnologia não possui a neutralidade devida, seja por motivo de engenharia social ou mesmo da autorreplicagem do aprendizado que as máquinas realizam, o que dificulta resultados previsíveis e resvala na discussão que orbita sobre a interface existente na capacidade da tecnologia aprender, e como constrói o processo decisório, e como isso pode ser empregado para fins políticos ou consumeristas.

A intencionalidade na manipulação decisória da população já pode ser observada a partir do uso da inteligência artificial nas redes sociais criadas para estimular os consumidores de produtos diversos, a partir do mapeamento realizado através de perfis de consumo e modos de vida, além das estratégias voltadas ao marketing e convenção de *insights* que estimulam o indivíduo a comprar.

Na mesma direção, as campanhas eleitorais cada vez mais agressivas do ponto de vista do estímulo a população para votar em determinado candidato, também utilizando-se de técnicas de inteligência artificial para direcionar os indivíduos a decisões político-partidárias, constituindo-se como grave violência política à sociedade e ainda, fragilizando o processo eleitoral democrático e com a lisura necessária a escolha livre e consciente.

Nessa direção, vem se desenhando um *Estado de Opinião* perigoso, no qual poderes políticos e governos vêm construindo nas plataformas de redes sociais, parâmetros mentais e formação de decisões a partir de inteligência artificial, cujas população vem sendo alvo levianamente, sem consciência participativa, tornando-se meros fantoches de um sistema criado para manipular opiniões. (BELLOSO, 2022)

Deste modo, é importante acompanhar e conhecer os processos que envolvem inteligência artificial e neurotecnologia, visando propor filtros e frenagem quando tais instrumentos de manipulação cerebral tornar-se perigoso para a livre criticidade da população.

A manipulação cognitiva cerebral que promova qualquer déficit ou carência na formação do livre discernimento das pessoas, sobre os fatos políticos e sociais, torna-se perigosa diante da necessidade de participação destas nas decisões da sociedade, portanto, força a construção do neurodireito para possibilitar o mínimo modelo garantista que vise proteger os indivíduos, das manipulações neurotecnológicas.

b) Risco de Desinformação Democrática (*Fake News*)

Como expõe Nuria Belloso (2022), todos possuem o direito a informação da *verdade*, direito ao conhecimento e informação com qualidade pois estes refletem o exercício de direitos fundamentais, contudo, há um grande desafio sobre este tipo de informação na internet atualmente, pois a recorrência da sua distorção é significativa, por vezes, comprometendo o processo decisório dos indivíduos, gerando vieses discriminatórios culturais, sexistas, consumeristas interferindo nos processos decisórios das relações sociais.

A disseminação de notícias falsas possui implicações sérias e negativas para a sociedade, posto que tais conteúdos são disseminados com velocidade, dificultando que os sistemas de checagem sejam acionados de imediato para evitar o compartilhamento de tais informações,tornando-se situação crucial e tecnicamente desafiadora no uso das redes sociais. (JOSÉ, KUMAR e CHANDRAN, 2021)

Tornou-se fenômeno significativo e que cuja doutrina e área de pesquisa emergente e incipiente que se apresentou como desafiador, em razão dos ínfimos recursos para se conhecer melhor como lidar com tal realidade, a exemplo da carência de dados, literatura acadêmica, estudos e experimentos; notadamente, uma falta de conhecimento das gerações passadas, posto que o fenômeno, na versão digital, é fruto deste momento histórico e cultural deste início de século.

As ferramentas de compartilhamento de notícias falsas, antes manuais, deram lugar às tecnologias de inteligência artificial e da robótica, com a massiva utilização de perfis de usuários construídos a partir do uso de tecnologias de algorítimos e *big data* e cruzamento de dados para desinformar.

A disseminação rápida e de modo massivo de informações não verdadeiras, visando alcance populacional e territorial para o fim de estimular determinados comportamentos sociais da população, passaram a ser vertente do ambiente cibernético.

Nessa direção, a concepção de como se denomina efetivamente as notícias falsas para o âmbito deste estudo é deveras importante, posto que esta não se confunde com outros elementos ligados a linguagem e o âmbito da informação, posto que pode levar o leitor ao conteúdo inadequado sobre o âmbito da informação.

Nesse sentido, a definição de notícias falsas ou *fake news*[55], são artigos de notícias intencionais e verificáveis, fabricados intencionalmente como artigos para serem compartilhados nas redes sociais; são originadas e categorizados em conteúdos diversos, alguns sites são inteiramente criados intencionalmente para tal finalidade enganosa, como também, há sites de conteúdos legítimos e, ainda, satíricos, que desinformam misturando fatos reais à falsidade informativa.

Muitos dos artigos também possuem origem na perspectiva satírica, mas, podem ser mal interpretados como se fossem factuais, especialmente, se vistos de modo isolado. Há que revelar, também, que as notícias falsas de sites enganosos possuem vida curta, como demonstrou os estudos das eleições dos EUA em 2016. (ALLCOTT e GENTZKOW, 2017)

[55] Apesar do termo *fake news* ser muito utilizado, o emprego adequado do termo é desinformação, segundo os especialistas.

Não obstante, nem todos os elementos ligados a informação são efetivamente falsas ou devem ser tidas como notícia falsa, como aduz Allcott e Gentzkow (2017), estão excluídas nessa denominação de *notícias falsas,* seis elementos inerentes aos erros, sátiras ou mentiras pessoais de agentes políticos, ou teorias da conspiração, portanto, sendo errôneo a inclusão no rol destes no modelo de desinformação.

Nesse sentido, não são notícias falsas, as informações não intencionais produzidas em um relatório com erro; rumores relativos a origem da notícia; informações ligadas as "*teorias da conspiração (estas são, por definição, difíceis de verificar como verdadeiras ou falsas, e são tipicamente originadas por pessoas que acreditam que elas sejam verdadeiras)".* (ALLCOTT e GENTZKOW, 2017; p.214)

As sátiras ou humor também não são notícias falsas, posto que não deverão ser interpretadas, como um fato verdadeiro; declarações falsas de políticos e relatórios tendenciosos ou enganosos, mas não totalmente falsos, portanto, notícias falsas são *distorção* e *não filtragem* da verdadeira informação. (ALLCOTT e GENTZKOW, 2017; p.214)

Quanto ao modelo utilizado para a disseminação de notícias falsas, este traz algumas dúvidas quanto a sua identificação, trazendo questionamentos sobre como se apresentam efetivamente, se diferente da mídia tendenciosa ou é uma forma inócua de entretenimento, sutil, através de filmes de ficção ou romances.

Nessa direção, o modelo desenhado[56] trouxe a tona no estudo sobre o *processo eleitoral dos EUA de 2016,* que cada empresa de marketing manipulava as informações de seus elegíveis através de estratégias de acompanhamento de relatórios, mapeando sinais do público alvo, e manipulando as notícias que publicavam.

Notaram dois estados distintos de manipulação da informação nesse processo eleitoral dos EUA sobre seus candidatos à eleição, demonstrando a compatibilidade entre o melhor desempenho daqueles, em razão da manipulação da gestora de mídia responsável e o trato de dados nas redes sociais.

No primeiro estado, a empresa de mídia ao recepcionar sinais sobre elementos informativos verdadeiros sobre seus candidatos podem diferir na precisão desses sinais, intervindo na informação plena, mitigando ou submetendo a exatidão; por sua vez, no segundo estado, a gestora midiática realizava investimentos dispendiosos para aumentar a percepção sobre o desempenho dos candidatos, ampliando a precisão dos sinais. (ALLCOTT e GENTZKOW, 2017)

[56] O modelo foi desenhado em 2016, por Gentzkow, Shapiro e Stone. (ALLCOTT; GENTZKOW, 2017)

Ampliando a análise sobre o processo de desinformação, o ataque a verdade da informação se divide em duas formas principais, indo além das notícias falsas que esta prefere denominar de *desinformação*, termo que esta acredita ser mais adequado para o que chama-se no senso comum de *fake news*, e o segundo modo, refere-se a discussão sobre *pós-verdade* no qual o conhecimento anteriormente concebido é relativizado. (BELLOSO, 2022)

Ambas as modalidades de afetação da informação verdadeira, enquanto direito fundamental, são prejudiciais a sociedade, pois fragilizam direitos e o principio democrático, constituindo-se segundo a professora Belloso (2022), como uma *infodemia*[57]; que tem como estratégia o lançamento de notícias falsas com compartilhamento veloz junto à população.

É importante notar nesse contexto que a discussão sobre *pós-verdade*, é utilizada para combater um conhecimento verdadeiro anteriormente concebido e consolidado pelos resultados da ciência ou provados pela experiência social, porém, estes são relativizados e postos à dúvida pública, levando a sociedade a desacreditar do conhecimento construído a partir de narrativas que beneficiam alguns grupos, em especial, no embate político-ideológico.

Para Belloso (2022), ambos os institutos que afetam a verdade informacional são bem distintos e merece ser objeto de discussão da sociedade, a *pós-verdade*, constitui-se uma distorção deliberada da realidade para manipular pessoas; enquanto que a *desinformação* conforma-se como a exposição de conteúdos falsos, mentirosos e desinformativos.

A desinformação e a pós-verdade são instrumentos que têm trazido grave prejuízo aos processos democráticos de países mesmo desenvolvidos, a exemplo do ocorrido nas eleições presidências dos Estados Unidos da América em 2016, nos quais *tweets*[58] disseminaram notícias falsas visando interferir nos resultados eleitorais daquela nação, cuja disputa principal ocorria entre Donald Trump e Bill Clinton. (BUDAK, 2019)

Na análise dos tweets que citavam os dois candidatos à presidência dos EUA, foi possível observar o impacto do conteúdo de notícias e as respostas abertas das entrevistas telefônicas, realizadas de modo nacionalmente representativas, destacando importantes lições inerentes aos consumidores de notícias e jornalistas, como retratou Budak:

> os produtores de notícias tradicionais superaram os produtores de notícias falsas em conjunto, (ii.) a prevalência de conteúdo produzido por editores de notícias falsas aumentou ao longo da campanha - particularmente entre os tweets que mencionaram Clinton, e (iii.) as mudanças nessa prevalência acompanharam de perto as mudanças na favorabilidade líquida de

[57] Alusão a uma pandemia de informações falsas;

[58] *Tweet* (inglês) refere-se a mensagens de até 140 caracteres publicados na rede social digital Twitter, de modo estrito, significa *pio de pássaro*, animal que representa o site. Disponível em https://www.significados.com.br/tweet/ acesso 28.05.2022.

> Clinton. Voltando ao conteúdo, identificamos (iv.) semelhanças e diferenças na definição. Voltando ao conteúdo, identificamos (iv.) semelhanças e diferenças na definição de agenda por meios de comunicação falsos e tradicionais e mostramos que (v.) as informações que os indivíduos mais comumente relataram ter lido, visto ou ouvido sobre os candidatos estavam mais alinhadas com o conteúdo produzidos por agências de notícias falsas do que por agências de notícias tradicionais, em particular para informações que os eleitores republicanos retiveram sobre Clinton. (BUDAK, 2019; p. 139)

Neste aspecto, também foram relevantes modelar a falsidade das informações a partir das características demográficas e compreender que as implicações para donos de plataformas, consumidores de noticias e jornalista precisa discutido por parte da sociedade civil. (BUDAK, 2019).

Especialmente, em razão dos riscos à democracia que tal manipulação da informação colocar acarretar e a possibilidade de por em xeque os aspectos inerentes aos processos eleitorais de países democráticos, que há anos já vinham se consolidando em perspectivas ligadas ao Estado democrático e constitucional de direito, torna o uso da inteligência artificial para manipulação decisória da população, ainda mais preocupante pelos resultados desastrosos que podem ocasionar.

É importante conceber, nesse contexto, que tanto a informação verdadeira quanto a informação falsa, em países democráticos como o Brasil andam sempre juntas, sendo necessário políticas sérias de enfrentamento, contudo, sendo perspicaz em relação aos aspectos da censura e da liberdade de expressão que precisam ser cuidadosamente mensurados, para que esta liberdade constitucional não seja gravemente afetada, na definição do que é ou não verdade pelo ente Estatal e entes midiáticos sob a escusa de proteção.

Há, sobretudo, o risco do poder Estatal passar a ser o único detentor da classificação da verdade no lugar da sociedade civil em sua trajetória e experiência decisória; tal tarefa estatal pode constituir-se filosófica e politicamente perigosa se direcionada a restringir apenas a verdade de alguns grupos de opinião, pondo em xeque as liberdades coletivas e individuais no crivo da verdade para a sociedade.

Como solução dessa realidade, algumas iniciativas já encontram-se em andamento de modo incipiente, as notícias falsas representam na internet um tipo específico de desinformação que também deve ser atacado por métodos automatizados ligados a análise de dados, se utilizando a mesma técnica do aprendizado de máquina para a prevenção ou repressão, visto que o *fake news* se tornou mais crítico nos últimos anos. (JOSÉ; KUMAR; CHANDRAN, 2021)

Diversas técnicas veem surgindo, entre elas o *deep learning* que refere-se à possibilidade de ensinar a máquina a detectar notícias falsas através do treino de diversos modelos de redes neurais artificiais, usando textos de artigos ou títulos de obras, que através de redes neurais artificiais e processamento de dados em várias camadas (hierárquicas), extraem os melhores níveis de dados, ensinando a máquina a avaliar e diferenciar o conjunto de dados, das informações falsas. (JOSÉ; KUMAR; CHANDRAN, 2021)

Nessa direção, é importante refletir sobre tais estratégias de desinformação e como estas interferem no poder decisório das pessoas para todas as atividades da vida humana, mas em especial, diante dos eleitores e do sufrágio universal que pode ser profundamente posto em fragilidade em razão da distorção das informações verdadeiras que as agências de mídia realizam.

As técnicas de gestão da mídia de candidatos as eleições, nos planos presidencial, estadual e municipal nunca forma tão afetados pela manipulação digital quanto neste início de século, e essa tendência refere-se a todos os partidos políticos e vieses político, revelando contudo, certa liberdade no poder de gerir informações por agências tendenciosas, de modo deliberado e até irresponsável.

A oferta de sinais de desempenho de candidatos por tais empresas *marketeiras* sobre os candidatos, do modo que lhes convém, contendo veracidade plena ou distorcida, lastreados pelos respectivos relatórios, de modo livre e influenciando a opinião pública ao passo em que mitiga o direito constitucional ao sufrágio em sua plenitude livre e democrática, precisa ser objeto de atenção.

Na mesma direção de cuidado, o parâmetro de definição do que é falso ou não quanto a informação, ainda é algo que a sociedade civil precisa se debruçar melhor, para a constituição de métricas coerentes que não envolvam a perda ou mitigação da liberdade de expressão, sob desculpa de atacar os riscos das redes sociais.

Apenas como incentivo a uma análise pormenorizada, o Tribunal Superior Eleitoral em meio ao processo eleitoral para presidente no Brasil aprovou *por unanimidade* resolução que dá a Justiça Eleitoral autonomia e poder de polícia para atuar de ofício diante de notícias falsas em sites e redes sociais, podendo ser retirada do ambiente virtual em até duas horas e sem a oitiva do Ministério Público Eleitoral. (TSE, 2022)

Entretanto, quanto à definição do que pode ou não ser considerado desinformação (*fake news*), a decisão não foi fruto de consenso no julgamento em plenário e em votação, 4 ministros foram favoráveis e 3 contra as notícias eleitorais em análise serem consideradas desinformação, fato que demonstra que ainda não há uma segurança jurídica sobre o conceito

do instituto no Brasil, portanto, trazendo questionamentos e riscos ao processo de liberdade de expressão, além da liberdade para o pleito eleitoral, como instrumento de cidadania.

Nesse sentido, a sociedade civil organizada conjuntamente com os Poderes constituídos da República, precisam ainda se comprometerem com a discussão sobre informação e desinformação de modo mais amplo, com a participação de atores múltiplos, para que a liberdade de expressão não seja em último caso, mitigada diante da dinâmica social e das forças políticas insurgentes, mesmo as forças dos próprios Poderes sobre os particulares.

4.2.9 Risco na Predição dos Algorítmos discriminatórios

A ação preditiva baseada em dados da população historicamente coletados e mantidos em banco de dados, selecionados de modo probabilísticos por meio de algorítmos e que levam a processos decisórios, por vezes, fundamentam-se em falhas e ruídos na informação, interferindo na igualdade social e racial.

Na tentativa de conceituação mais aprofundada do que seria essa tarefa *preditiva*, cabe informar que ainda há uma confusão na doutrina sobre o instituto, dado ao fato de englobar recursos técnicos computacionais desafiadores para a compreensão filosófica plena.

Como informa Provost (2013, p.22) a *predição* é a quantidade massiva de dados analisados por meio de uma técnica para estimar valor desconhecidos, por meio de algorítimos matemáticos; não obstante, não possuir ambiência conceitual específica.

Senão, tem a predição a função de *predizer*, *antecipadamente*, *uma conduta provável* a ser realizada pelo indivíduo, a partir da formação de perfis de conduta de outros indivíduos, registrados historicamente em um banco de dados, que passam a fundamentar a tarefa matemática dos algorítmos com base em registros passados.

As informações projetadas pela máquina, através de algoritmos e de modo probabilístico matemático, geram uma determinação preditiva sobre ações futuras, condutas prováveis a serem cometidas por indivíduos, mas que podem ser falhas estabelecendo vieses discriminatórios, seja a apartir da qualidade do banco de dados viciados com diversos elementos discriminatórios, quanto pela qualidade do próprio algorítmo.

Logo a decisão é preditiva, quando explora os dados e informações das bases de dados mediante critérios pautados na experiência passada, de modo histórico e por meio da estatística busca alcançar ou responder um objetivo do engenheiro computacional.

A tarefa se faz por meios dos dados dos usuários existentes no banco de dados e se relacionam a informações diversas como os critérios de raça, cor, idade, conduta, local de moradia, condição econômica, cujo resultado probabilístico tende a emitir um resultado que antecipa um risco e passa a pautar decisões no plano fático e real, concedendo ou não direitos ou restringindo liberdades, por vezes apresentando decisões erradas.

Como retrata Llinares (2020), a antecipação proposta pelo modelo preditivo é uma utopia, sendo uma amplificação da *cientificização* das atividades de cruzamento de dados para determinar o futuro; fato que torna a técnica da predição totalmente frágil, na tentativa de determinar como um indivíduo se comportará, em razão de possuir determinadas características ou fazer parte de determinado grupo, no banco de dados.

Há que reconhecer que na predição embora nao seja possível (e nunca é possível) prever a realização de crimes, esta técnica auxiliar na identificação de probabilidades quanto a eventos futuros com base no aprendizado sobre os eventos passados, permitindo a adoção de estratégias de prevençao e redução das condicionantes delitivas. (LLINARES, 2020; 6/7)

Funciona nesta concepção, de modo utópico, uma utopia da antecipação que amplifica o otimismo sobre a tarefa, posibilitando como ponto positivo a gestão mais eficiente dos recursos policiais e menos subjetividade decisória, mas que nao pode se distanciar das demandas públicas por justiça e responsabilização, devendo ser usada para corrigir o preconceito no tratamento discriminatorio dos grupos sub-representados. (LLINARES, 2020)

O grande problema que envolve o modelo preditivo na sociedade, entretanto, é justamente em razão das desigualdades estruturais e históricas que o Brasil apresenta (como em outros países) e das preocupações sobre as informações dispostas nos banco de dados brasileiros que alimentam os sistemas de monitoramento e cruzamento de dados sensíveis da população, como por exemplo, os registros existentes historicamente no sistema criminal que culminam na discriminação da população negra e pobre.

Nessa direção, Bogard (2012, p. 36-37) reflete que a sociedade fica refém da conexão de máquinas computacionais e dos sistemas de vigilância com um alcance considerável, através da constituição de lógicas construídas por meio do acúmulo de dados dos usuários, que dependem da sua qualidade.

Portanto, dados incompletos ou fragmentados que alimentam o sistema e impossibilitam a construção de banco de dados sólido e seguro sobre diversas categorias criminais, podem interferir negativamente e construir categorização discriminatória no banco de dados, mesmo que de modo não intencional, visto que as informações tornam-se seletivas e

direcionadas a um público ou grupo, em razão da dinâmica social e formas de alimentação inadequada. (FERGUSON, 2017)

Assim, os resultados das pesquisas preditivas e probabilísticas emanam riscos quanto a construção do algorítimos matemáticos, que farão a seleção de dados, posto que estes são criados por seres humanos, que acumulam processos discriminatórios da sociedade.

Além do risco relativo aos bancos de informações que podem ter baixa qualidade, dados incompletos ou categorizados para determinar condutas de determinados grupos vulnerabilizados ao longo do tempo, que podem fundamentar erros de sistema ou erros humanos, replicando informações erradas, em especial, dentro do modelo preditivo voltado à prevenção do crime. (FERGUSON, 2017)

Nesse âmbito, a inteligência artificial, algorítmo e *big data* nas tarefas do âmbito da segurança pública e no âmbito da justiça criminal e do judiciário, bem como, no monitoramento social, pode trazer sérios problemas relativos à ocorrência de discriminações.

Tais riscos precisam ser prevenidos na aplicação das tecnologias no processamento de informações, haja vista, tenderem a serem desastrosas do ponto de vista da evolução dos direitos humanos no mundo, fragilizando o legado conquistado ao longo do tempo da humanidade.

A alimentação do banco de dados de modo incorreto e por algorítmos tendenciosos, ainda que de modo não proposital ou sem supervisão adequada, pode tornar o sistema probabilístico preditivo uma armadilha social e fonte de erros desastrosa do ponto de vista do controle social, permitindo vieses tendenciosos que podem interferir na dignidade da pessoa humana. (XAVIER, 2020)

a) Risco no Controle Social Preditivo

A possibilidade de afetação de grupos vulneráveis ou sub-representados nesse modelo preditivo de controle social, segundo Llnares (2020), pode ainda ser incrementado pela manipulação de dados para fins político-ideológicos, a partir de análises estatísticas e cálculos de probabilidade, tornando o instrumento preditivo ainda mais preocupante.

Assim, a utilização do modelo preditivo apesar de evidenciar uma automatização interessante na dinâmica social e diante da enorme quantidade de dados a se processar, este pode se tornar perigoso se o desenvolvimento de sistemas inteligentes baseados em autoaprendizagem das máquinas levarem a identificação de condutas possíveis, por indivíduos que não necessariamente, a realizariam, predizendo ações que jamais seriam cometidas.

Nesse sentido, há dois direitos que entram nessa discussão, que é o direito fundamental à segurança e o direito fundamental à privacidade e, apesar de no Estado democrático de direito, se demonstrarem por vezes de modo conflituoso, pois há o dever estatal de promover a segurança, e por outro lado, há o dever também de se abster no que tange a privacidade dos cidadãos, ou ainda, de atuar para promover a liberdade sobre a vida privada; contudo, não há real conflito.

O que existem em verdade, é que deve haver um sopesamento de direitos fundamentais, nas situações concretas, que permita de modo equilibrado que um ou outro direito atue para proteger o cidadão, em especial, diante dos direitos da coletividade, que deve de modo totalmente pacífico, prevalecer.

É condição *sine qua non*, que o Estado possa efetivamente atuar no controle e vigilância social, de modo não indiscriminado e sim, igualitário e sem abusos; tão pouco, a sociedade civil não pode concordar com a implementação de tecnologias de inteligência artificial na segurança pública de modo que venha a ferir à liberdade coletiva, notadamente, o que se espera é a construção de freios e contrapesos que permitam a participação da sociedade nas construção dos instrumentos legais para uso de tais tecnologias.

A proteção dos dados no desenvolvimento da segurança cibernética diante do direito à privacidade e à proteção dos dados sensíveis, precisa encontrar o ponto de equilíbrio que limite um instituto diante do outro, assim, promovendo o uso da inteligência artificial por entes privados e pelo próprio Estado, de modo adequado e ético socialmente.

Defende-se que tais conformações institucionais precisam ser bem construídas para produzir segurança à sociedade, sem ferir a dignidade da pessoa humana em sua máxima expressão. A construção coletiva, por exemplo, entre instituições do sistema criminal com a sociedade civil pode ser um caminho produtivo para novos desenhos pensados à luz da dignidade humana.

O mecanismo preditivo mal alimentado abre margem às tais concepções tendenciosas de discriminação pautadas em ideologias diversas, com resultados racistas e pautados na seletividade do sistema penal, que no Brasil já é historicamente existente em razão dos negros e pobres serem os destinatários principais das políticas públicas de encarceramento de massa.

Ocorre, porém, que tais disposições futuras são de fato previsões utópicas, fantasias, que não se reproduzem comprovadamente na realidade, logo, tais cadeias interconectadas operam mera simulação, mas vem adquirindo uma função central no processo decisório das organizações, das polícias e dos governos.

Esta técnica traz incerteza aos processos de prevenção da criminalidade e da troca de informações no âmbito do controle social, sendo grande o risco de erro a pesar de haver pontos positivos que estas tecnologias apresentam ao processar grande quantidade e qualidade de dados, quando se deseja fazer o controle social.

O modelo preditivo permite potencializar a seletividade racial histórica que já está presente na política criminal tradicional brasileira, com riscos de conceber a mesma realidade observada nos Estados Unidos da America (EUA), cuja implementação desta experiência revelou o monitoramento de grupos específicos, como tarefa pública.

Deste modo, as técnicas de IA ligadas ao vídeomonitoramento, geolocalização e reconhecimento facial, permitiram um salto evolutivo no trabalho preditivo das maquinas, posto que o cruzamento de dados da máquina unido à projeção física de localização dos indivíduos e dados biométricos que possibilitaram acesso a uma gama de informações da intimidade a serem administradas pelos entes estatais.

Há de fato o risco de invasão da privacidade das pessoas comuns, da afetação da intimidade, do endereço e da moradia das pessoas, de tais informações serem utilizadas para fins coercitivos em condutas diversas, com o condão de vulnerabilizar o ser diante de perseguições políticas ou econômicas, pondo em risco a própria vida individual a partir da vulnerabilidade da sua localização e formas de vida, a apartir do controle social.

b) Risco dos Algorítmos como Política Criminal e de Polícia Preditiva

Polícia preditiva é a utilização da probabilidade proporcionada pelos algorítimos, selecionando dados históricos de antigos delinquentes, para determinar possíveis perfis de pessoas aptas à produção futura de novos crimes, de modo probabilístico e antecipado, ou seja, preditivo (pautado em uma previsão futura) quanto à ocorrência de criminalidade.

Como retrata Fernando Miró-Llinares (2020) sobre a polícia preditiva, "*embora não possa (e nunca possa) prever a perpetração de crimes, ajuda a identificar a probabilidade de eventos futuros [...]. Assim, permite a adoção de estratégias preventivas para fins de prevenção, redução ou mitigação delitiva.*".

Porém, esse modelo que opera semelhanças históricas, pode se tornar permissivo em alguns pontos, ocasionando uma série de discriminações no âmbito penal, mas também pode favorecer redução de subjetividades por parte das ações policiais no plano social.

Há, contudo, que evidenciar pontos positivos desta tecnologia que emprega algorítimos e inteligência artificial na política criminal, segundo Llinares (2020):

> Os benefícios da tecnologia também vão além da prevenção do crime, por exemplo, na gestão mais eficiente dos recursos policiais e menos subjetividade na tomada de decisão policial. A capacidade dos algoritmos de processar grandes quantidades de dados permite que eles avaliem mais informações mais rapidamente do que qualquer policial, analista criminal ou departamento individual jamais poderia. Em um momento de crescentes demandas públicas por justiça e responsabilidade, isso se torna um valor em si. Além disso, essas ferramentas poderiam corrigir o preconceito humano ao superar o tratamento discriminatório historicamente sofrido por vários grupos sub-representados. (LLINARES, 2020, p.6/7)

Diante da discussão da melhor adequação para uso dos algorítmos na política criminal, os estudos sobre *Polícia Preditiva* de Xavier, Portalés, Guimarães e Farias (2022), reforçam a necessidade de observar que a adequadação desta técnica preditiva torna-se dependente de *dois elementos fundamentais* que podem permitir ou não, o sucesso da técnica.

O primeiro elemento refere-se a margem de *falibilidade* da técnica preditiva, devendo ser considerado que a qualidade do algorítmo é diretamente proporcional aos critérios empregados pelos engenheiros computacionais na sua criação, treinamento e desenvolvimento, portanto, estando íntimamente ligados a definição dos indicadores *não viciados ou discriminatórios* que basearam o trabalho algorítmico. (XAVIER, PORTALÉS, GUIMARÃES e FARIAS, 2022)

E o segundo elemento, se relaciona a compreensão sobre o nível de *acurácia e exatidão* dos resultados expostos pela máquina, no trabalho preditivo; nesse sentido, dependente da compatibilidade do modelo de algorítmo empregado para determinada tarefa e objetivo, cujos códigos-fonte e modelos de processamento de dados devem ser transparentes e à mostra para a sociedade. (XAVIER, PORTALÉS, GUIMARÃES e FARIAS, 2022)

Não obstante, muitos algorítmos atuam com *opacidade* e sem transparência, apresentando, por vezes, uma espécie de *caixa-preta* que não permitem sua analise adequada e geram duvidas sobre o modo de processamento das informações, em especial, nos modelos de algorítmos, como os do tipo bosques aleatórios ou redes bayesianas e os de tensor flow, demandando maior transparência da empresas a sociedade em geral. (XAVIER, PORTALÉS, GUIMARÃES e FARIAS, 2022)

O grande risco dessa *opacidade* dos algorítmos é que os sistemas de Inteligência Artificial podem produzir "*arbitrariedade de critérios e de conclusões, associada à discricionariedade, à discrepância com direitos fundamentais e outros princípios jurídicos,*

associando o sistema ao aprofundamento da desigualdade e imprevisibilidade[...]", a partir de perfis e compreensões automatizadas. (HARTMANN PEIXOTO, 2020; p.28)

Comportam essa análise duas observações relevantes: a primeira de que *os riscos são controláveis* se o sistema de IA for bem estruturado sob fundamentos éticos robustos; e a segunda, que se refere ao *comportamento humano,* visto que este já apresenta riscos naturalmente, portanto, acredita-se que a diferença entre o resultado cognitivo artificial e o do ser humano, está na possibilidade do comportamento artificial ser mais facilmente corrigido quanto aos desvios, diferentemente da condição humana. (HARTMANN PEIXOTO, 2020)

Não obstante, as correções precisam ser realizadas com transparência quanto aos algorítmos diante da atividade de policía preditiva, demandando, fiscalização, acompanhamento e monitoramento humano permanente, juntamente com a garantía de que um sistema robusto e alto nível de confiabilidade, com resultados previsíveis será estruturado, entretanto, a crítica parte de que tais elementos ainda não chegaram nesse nível de aplicação.

Portanto, neste estágio da técnica preditiva, e considerando o quadro histórico do Brasil cuja população carcerária é constituída eminentemente de negros, historicamente concebida pela reprodução de desigualdades sociais de classe e de raça, entre negros e não-negros, recomenda-se cautela nessa técnica de polícia preditiva para o Brasil.

Ademais, relembrar que a Administração Pública deve atuar para reduzir o quadro de exclusão social, prevenindo delitos e promovendo emancipação social, e não ao contrário, é sempre importante; afinal cabe ter o cuidado para a sociedade não estar implementando novos mecanismos de controle da população jovem, negra e pobre, com fomento as desigualdades raciais, sob a escusa de desenvolvimento econômico e social.

Para fins comparativos quanto aos problemas e desafios a serem enfrentados na temática da política criminal, o modelo de Polícia Preditiva implementada nos Estados Unidos da América serve de inspiração, do que *não se pode* realizar no plano pátrio.

Os EUA foi uma nação que efetivamente aplicou um programa de polícia preditiva com foco na prevenção da criminalidade, utilizando banco de dados e o mecanismo de algorítmos a partir dos dados sensíveis para análise no âmbito da política criminal e teve como objetivo inicial, reduzir a violência *contra grupos vulneráveis*, em especial, dos crimes que ocorriam *em face da população negra* daquele país.

O programa norte americano foi denominado como reforma por meio da polícia preditiva (*predictive police for reform*) e visou a reformulação das instituições policiais, das Polícias, para que se tornassem mais cientificas, técnicas e mais objetivas no trato de dados sensíveis da população, para prevenção do crime.

O intuito inicial foi uma atuação *menos preconceituosa pela polícia* face ao público negro, utilizando para tal premissa, os componentes de dados algorítmicos preditivos e probabilísticos de criminalidade, contudo, o contrário foi evidenciado.

Tomando por base locais de execução de crimes, que giravam em torno de determinadas comunidades econômica e socialmente desfavorecidas, fato que levou a resultados preditivos baseados nos novos dados geográficos especializados, estes serviram para reforçar que determinado local era mais violento que outro, gerando resultados que desfavoreciam comunidades pobres em relação a outros espaços econômico e socialmente mais favorecidos. Tais distorções em verdade foram criadas unicamente em razão das informações passadas ao banco de dados.

Para Shapiro (2019, p.456-548), a possibilidade de falhas desse mecanismo preditivo foi grande em razão da incapacidade de tal sistema ser tão objetivo, apresentando indeterminações do sistema em razão da alimentação com base em abordagens físicas anteriores, gerando uma série de incompreensões ao sistema algorítmico, que distorcia a capacidade adequada de medição de potenciais criminosos de modo real.

A performance dos registros e dos resultados algorítmicos segundo Shapiro (2019), somente poderiam produzir predições adequadas, se a alimentação da base de dados fossem fidedignas na realidade criminal, contudo, as abordagens concentradas em determinadas regiões, geravam efeitos reativos a potenciais criminosos de tal área, retroalimentando os dados do banco de dados de modo viciado e preconceituoso.

Na segunda experiência norte americana, a utilização do conhecido como algorítmo *COMPAS*, utilizado para gerar pareceres técnicos sobre progressão de regime de prisão nos Estados Unidos, o banco de dados de algoritmos apresentava uma serie de conteúdos incompletos sociais e raciais, além de se valer de dados policiais antecedentes dos indivíduos para opinar sobre o pedido do paciente, que em boa parte tinham resultado negativo. (WADSWORTH, 2018)

Observou-se que há a necessidade de melhor regulação desses instrumentos algorítmicos, e até mesmo, de como são construídos, de modo a regular e limitar a extensão e alcance do uso de dados sensíveis para aplicação das técnicas de polícia preditiva, notadamente, para que a ação de entes privados e estatais como ocorrida nos Estados Unidos, não sejam aplicadas no Brasil.

No âmbito pátrio, os modelos de cibersegurança estão utilizando de sistema preditivos no tocante a utilização de inteligência artificial na seleção de processo judiciais, na saúde em razão da pandemia, no sistema de pagamento de benefícios de assistência

governamental, para gestão de pessoas na administração pública, e na área penal, por meio de vídeomonitoramento com reconhecimento facial cruzados com o banco de dados da justiça, contudo, com riscos inerentes a carência de instrumentos éticos regulatórios, bem discutidos pela sociedade.

c) Risco de julgamento preditivo no Poder Judiciário (Robôs)

A expansão da inteligência artificial e da robótica no Poder Judiciário, justiça *preditiva*, vem sendo uma realidade que tem trazido muitos positivos no tocante a seleção e organização de dados processuais, porém, também comporta diversos riscos diante da nova tecnologia que permite certa facilitação no processo decisório do juiz, inclusive, sobre o mérito jurídico, mas que não deve ser utilizado, sob pena de ferir direitos fundamentais.

Note-se que apesar da tecnologia já estar sendo implementada de modo veloz e se espalhando-se pelo país, não há uma regulação geral sobre decisões judiciais pautadas preditivamente nos resultados robóticos ou dos algorítimos utilizados no Poder Judiciário, existe sim, um projeto de lei nacional em discussão, e um documento *ético* que começa a delinear alguma regulação do instituto para o Poder Judiciário.

Considerando que ainda caminha-se para uma regulação efetiva geral sobre IA no Brasil, por dever de cuidado, é importante relembrar que a força constitucional no tocante a possibilidade do *julgamento de mérito preditivo* por máquinas, é de todo proibido no ordenamento brasileiro, haja vista, ferir princípios relevantes como o do juiz natural, do livre convencimento do juiz e do devido processo legal.

Mas, é importante compreender que do ponto de vista técnico e de máquina tal assertiva alega-se ser plenamente possível e conceda decisões, não obstante ser questionável a qualidade desse resultado para o efetivo *senso de justiça,* a partir da reflexão judicial pautada na isonomia e equidade social.

Acrescente que nos experimentos realizados em 2017, realizados pelo Ministério da Justiça da França, ao testar um software para *justiça preditiva* a partir de processos em fase recursal de decisões civis, sociais e comerciais, a conclusão foi de que a tecnologia jurídica baseada em inteligência artificial, não possuía o valor agregado do trabalho reflexivo de um *juiz de verdade*, portanto, "*levaram a resultados aberrantes ou inadequados"* em razão de confusões lexicais e de causalidade na forma de pensar dos *juízes robô.* (CEPEJ, 2018)

Ademais, a tecnologia de inteligência artificial não se constitui um elemento homogêneo, tendo o condão de levar as decisões judiciais a uma relação de autoaprendizagem

constante que modifica suas premissas futuras, preditiva, com base em banco de dados; assim, sob duas técnicas principais: o processamento da linguagem natural e da aprendizagem automatizada. (CEPEJ, 2018)

Do ponto de vista acadêmico, não há nessa tarefa o mero desejo de reprodução do raciocínio jurídico, mas a da interação entre diversos parâmetros para conceber uma decisão, aprendendo automaticamente novos modelos, reinventando-se a todo instante, "*esses modelos seriam então utilizados para 'predizer' ou 'prever' uma futura decisão judicial",* dependente da confiabilidade do modelo, por sua vez, da qualidade dos dados utilizados nesse fenômeno preditivo. (CEJEP, 2018).

No plano fático sobre a IA na justiça do Brasil, há pelo menos cinco robôs baseado em inteligência artificial e algorítimos e com a tecnologia de *big data*, que já estão sendo empregados em tarefas do Poder Judiciário, criados para finalidades próprias, defendidas como organizativas, de modo ampliar o desempenho e a agilidade processual.

Como revela Atheniense (2018, p. 158), é necessário compreender que precisamos "*admitir que sequer atingimos de fato experiências maduras para apurar com isenção os riscos, benefícios e limites de conformidade ética e legal dessa nova cultura digital";* contudo, é necessário construir o mínimo de condições de análise legal para que tais tecnologias subexistam com o mínimo de legalidade.

Da expansão dos robôs o que se apresenta atualmente é que os principais robôs implantados desde 2017, baseados em inteligência artificial no Judiciário brasileiro são: o *Pôti* (TJRN)[59] criado para realizar execução fiscal e penhora de bens; o *Elis* (TJPE)[60] que faz triagem de processos de execução fiscal, equivalentes a 53% de todas ações naquele tribunal.

O robô *Radar* (TJMG)[61] que auxilia juízes a localizar processos repetitivos e agrupá-los, fornecendo recursos para casos similares. (AMARAL, 2020)

Também, há o *Sinapses*[62] do (TJRO)[63] regulado na mesma resolução 332/2020, que faz uso de "*redes neurais e possui banco de dados com 44 mil despachos, sentenças e julgamentos, e seleciona decisões anteriores sobre o mesmo tema*", auxiliando na elaboração de textos. (CNJ, 2020)

---

[59] TJRN - Tribunal de Justiça do Rio Grande do Norte;
[60] TJPE - Tribunal de Justiça de Pernambuco;
[61] TJMG - Tribunal de Justiça de Minas Gerais;
[62]Sinapses é uma plataforma virtual que permite *"solução computacional, mantida pelo Conselho Nacional de Justiça, com o objetivo de armazenar, testar, treinar, distribuir e auditar modelos de Inteligência Artificial;"* (CNJ, 2020)
[63] TJRO -Tribunal de Justiça de Rondônia;

E o *Victor* (STF)[64], criado para classificar peças processuais, sugerindo passos do processo ao magistrado (AMARAL, 2020).

Como retratam Maia Filho e Junquilho (2018; p.222) o projeto Victor, nome em homenagem ao ex-Ministro Victor Nunes Leal[65], prevê que a máquina promova o aprendizado computacional em IA com a finalidade de realizar *"o juízo acerca da repercussão geral no STF, avaliando a totalidade dos recursos extraordinários e agravos em recursos extraordinários que chegam à Corte*".

Logo, além do trabalho de investigar se tais processos cumprem o mandado do art. 102, § 3º, da Constituição Federal, que vincula a análise ao tema de repercussão geral, o robô também faz juízo no sentido dessa repercussão, excluindo automaticamente processos que não se enquadrem nas especificações.

O objetivo não é a decisão final a cerca da repercussão, mas que a máquina atue em camadas de organização dos processos[66], analisando os recursos e os temas relacionados de forma mais clara e consistente. (MAIA FILHO; JUNQUILHO, 2018, p.222)

Se de um lado há uma contribuição para a dinâmica organizativa e de seleção de processos, por outro ainda é necessário "*a elaboração de arcabouços legais e de regulação ética sobre a matéria faz-se urgente, pois são inegáveis, no mundo atual, os impactos sociais e culturais do desenvolvimento tecnológico centrado em dados"* (MAIA FILHO; JUNQUILHO, 2018, p.225)

Nessa direção, o Conselho Nacional de Justiça tornou-se o primeiro órgão a criar o primeiro regramento ético para utilização da inteligência artificial no Brasil, e sendo ele específicos para o âmbito do Judiciário (CNJ, 2020).

A iniciativa louvável surge em razão dos riscos evidenciados pelo órgão, no uso preditivo e seletivo desta tecnologia para julgamento e decisão jurídica, posto que não podem se afastar das premissas da dignidade da pessoa humana, logo, os riscos existem e são relevantes a todos da sociedade e o CNJ foi pioneiro, de modo a prevenir tais riscos.

É importante que a tarefa jurisdicional tenha o condão de prevenir paralelo a decisão da lide, a construção de sentenças judiciais discriminatórias ou pautadas na seletividade racial,

---

[64] STF - Supremo Tribunal Federal;

[65] Ministro entre 1960 a 1969, responsável pela organização da jurisprudência do STF em súmulas;

[66] Em encontro técnico entre servidores dos Tribunais de Justiça da *Bahia (TJ-BA) e de São Paulo (TJ-SP)* foram discutidas *"aplicação de inteligência artificial e automatização nos processos judiciais"*, com o objetivo de promover celeridade na tramitação processual e auxiliar os magistrados e servidores na rotinas judiciais; reforçou-se inclusive, que o Tribunal de Contas do Estado da Bahia (TCE-BA), já desenvolveu modelo preditivo, com emprego de inteligência artificial focada nas auditorias dos convênios, tendo realizado a implantação desta tecnologia em 2022. (TJBA, 2022)

sendo este o grande alerta que esta porção da pesquisa pretende submeter ao leitor, a limitação ética e principiológica, por que não dizer, *prima facie* que os instrumentos tecnológicos devem se submeter.

Deste modo, os instrumentos preditivos aplicados ao judiciário pautados em IA, que formulam antes de tudo resultados matemáticos e probabilísticos, baseada em banco de dados históricos e algorítmicos devem prevenir o impacto negativo às decisões judiciais, estas que por sua vez, não devem ser automatizadas sob pena de quebrar o sistema de equilíbrio da jurisdição, até mesmo, do contraditório e do livre convencimento do juiz.

Há aqui três preocupações distintas a serem analisadas de modo específico, a primeira que se refere ao produto probabilístico criado pela máquina sugerindo um resultado jurídico, notadamente *baseado no histórico da base de dados* (bem ou mal formado) que influenciará no resultado futuro.

No caso do Brasil, o conjunto de dados do âmbito penal ao longo dos últimos 130 anos pós-escravidão, podem levar a elevada discriminação racial ainda nos dias atuais, posto que os registros de criminalidade do sistema penal e carcerário brasileiro ainda se demonstram seletivos e viciados, em razão de terem sido construídos historicamente desde a escravização dos negros, apresentando ainda hoje, as maiores estatísticas de criminalidade no país[67].

Nesse sentido, o banco de dados pautado na postura seletiva e discriminatória em relação aos negros no Brasil desde o período escravocrata, favorece resultados preditivos com probabilidade para penalizar esse público negro, logo, podendo conceber um instrumento preditivo perigoso para estes grupos de usuários no sistema, por exemplo.

Na segunda dimensão, há o elemento da *independência decisória do Juiz* diante da sugestão da máquina, na formação do convencimento, que pode permanecer *livre ou não*, diante da sugestão produzida pela inteligência artificial e a depender de a construção da sentença e efetivação da jurisdição ocorre.

Esta autonomia decisória do Juiz se faz deveras importante posto que, atrelado ao caso concreto determina uma atuação independente da máquina, que lhe serve como mero instrumento de organização de dados, mas, não de decisão.

---

[67] De 1992 a 2013 o encarceramento no Brasil aumentou por volta de 317,9%**,** no qual os pretos e pardos (negros) correspondem a 60% dos detentos, demonstrando seletividade racial no sistema penal; os **d**ados estatísticos podem ser acompanhados no site do Ministério da Justiça e Conselho Nacional de Justiça (Mapa das prisões) e através do *Kings College* de Londres, centro internacional para estudo das prisões. Disponível em https://www.prisonstudies.org/. Acesso em 02 Mai 2022.

É Claro que os juízes não estão autorizados a utilizar a máquina para realizar julgamentos quanto ao mérito dos processos em andamento com robôs, a menos que desconsiderem o distinguir (d*istinguishing)* e anular *(overruling), e* utilizem resultados traçados por algorítimos, fato que seria muito perigoso no ordenamento jurídico.

Portanto, a decisão *livre* do juiz é necessária e insubstituível, pois permite analisar o processo dentro de sua complexidade subjetiva cerebral, também passível de discriminações, contudo, pautada em uma espécie de "*feeling"*[68] humano.

Refere-se além da postura da imparcialidade, a uma *porção cerebral ímpar do ser humano*, que a máquina ainda não pode copiar e não pode ser superada pela racionalidade matemática da máquina, logo, permite o trabalho da jurisdição e do processo decisório judicial, pautado na equidade, quando liberdades e direitos individuais ou coletivos são posto em xeque no caso concreto.

E a terceira dimensão, é sobre o questionamento realizado por Xavier (2021, p. 135), "*se é possível empregar a justiça preditiva para detectar condutas por parte dos juízes que podem configurar prevaricação judicial?"*

Responde que a resposta é positiva e existem diversos mecanismos úteis para esta finalidade, se referem a sistemas de predição de sentença que servem para que os magistrados decidam com maior consciência e responsabilidade na mudança das jurisprudências, contudo, os erros judiciais em relação as vítimas e as detenções injustas, não serão evitados com esta técnica. (XAVIER, 2021; p.135)

Deste modo, tecer sobre a implantação de sistemas de justiça preditiva no judiciário compreende dois questionamentos que manifestam prudência na analise: primeiro no modo como são construídas as sentenças judiciais, e no segundo ponto, como são analisados os comportamentos das autoridades judiciais no processo. (XAVIER, 2021)

Portanto, diante de tais preocupações, o desenho de um modelo penal e de administração da justiça, não é tão importante diante da implementação das tecnologias pautadas na inteligência artificial. (XAVIER, 2021)

O grande impacto está na esfera processual e da responsabilidade administrativa, que podem ser fragilizados diante de tais sistemas preditivos, a depender de como se constroem as decisões e de como atua o juiz, tornando a tarefa processual o grande elemento diferenciador no sistema preditivo judicial, portanto, não pode haver desídia diante desta análise processual.

[68] Categorizados genericamente como "*Feeling",* sentimento ou pressentimento humano.

Demanda na necessidade de organização de uma carreira judicial independente que se paute na plena submissão à lei e ao direito, pautadas em garantias fundamentais, como retrata Xavier (2021), compreendendo a importância da garantia da jurisdição.

> Hay que entender que el proceso es una garantía de la jurisdicción, por ello sirve para eliminar el automatismo de las sentencias, de las decisiones adoptadas al sabor de los aforismos individuales y de las pasiones. El proceso es el instrumento básico para asegurar la contradicción, la producción de pruebas, la igualdad de las partes y el sometimiento pleno a la ley y al derecho por medio de un procedimiento con todas las garantías y de una sentencia motivada, congruente y revisable en vía de recurso. (XAVIER, 2021; p. 137) [69]

Discussão, portanto, que tem como elemento de destaque os direitos fundamentais diante do uso da inteligência artificial no Poder Judiciário, cujos olhares devem estar voltados a adequada formatação ou desenho, justamente neste momento histórico, em que as técnicas dos algorítmos, *big data*, dados em nuvem e robótica vem crescendo no âmbito processual, clamando pela melhor modelagem de jurisdição.

4.2.10 Risco de Guerra Cibernética

A criminalidade cibernética abriu um caminho perigoso para prejuízos econômicos e sociais com dimensões ainda maiores que os habituais crimes inerentes à segurança da informação, podendo afetar direitos fundamentais coletivos relevantes, em caráter global, e humanitário com o uso de inteligência artificial, algorítimos e robotização de estratégias da informática.

A possibilidade de ocorrência de *guerras cibernéticas* entre Estados soberanos que até pouco tempo encontrava-se no âmbito da mera cogitação e risco, passou do plano da presunção para a realidade, demonstrando exatamente neste momento histórico, um novo domínio de guerra que difere do exclusivo emprego de armamento bélico e dominação territorial.

---

[69] Tradução livre: "Há que entender que o processo é uma garantia da jurisdição, por isto serve para eliminar o automatismo das sentenças, das decisões adotadas ao sabor dos aforismos individuais e das paixões. O processo é o instrumento básico para garantir a contradição, a produção de provas, à igualdade das partes e o estímulo pleno à lei e ao direito por meio de um procedimento com todas as garantias e de uma sentença motivada, congruente e revisável em via de recurso."

Do ponto de vista da conceituação, não há um consenso sobre a definição de *guerra cibernética*, sendo esta uma construção mais sociológica associada à concepção de guerra entre estados soberanos no ambiente cibernético, visando fragilizar uma nação autônoma, por meio de ataques virtuais e incidentes cibernéticos explorando sistemas de tecnologia e informações alheias.

Como retrata P. W. Singer a guerra cibernética, ciberguerra ou *cyberwar*, pode se definir como o emprego de ataques digitais por um Estado soberano para prejudicar os sistemas de computadores de outro país ou nação, visando gerar danos significativos, comparáveis à guerra real, tradicional.

Para o Ministério da Defesa do Brasil, Guerra Cibernética é:

> o conjunto de ações para uso ofensivo e defensivo de informações e sistemas para negar, explorar, corromper ou destruir valores do adversário baseados em informações, sistema de informação e redes de computadores. Essas ações são elaboradas para obtenção de vantagens tanto na área militar quanto na área civil. (BRASIL, 2007; p. 123).

Nesta concepção militar, na guerra cibernética se concebem operações que exploram capacidades cibernéticas para ter domínio da informação ou reduzir a capacidade de resposta do oponente, dentro do ambiente cibernético ou fora dele, incluindo ataques pela internet às redes de telecomunicações, sistemas de computadores, processadores e controladores; gerando um ambiente operacional abrangente e *lato* de Guerra Cibernética. (LEITE SILVA, 2014)

Nessa modalidade de guerra os opositores se aproveitam do anonimato, da surpresa, da incerteza e do disfarce, além da inexistência de barreiras físicas para cometimento de agressões, estes se aproveitam das vulnerabilidades dos sistemas (assimetrias) para explorar fragilidades das nações, que segundo Leite Silva (2014), ultrapassa o âmbito virtual e pode produzir efeitos no mundo real, cinético, com eficácia e sucesso.

As cogitações iniciais sobre a possibilidade de guerra cibernética giravam em torno dos Estados Unidos da América (EUA) e China, que já tencionavam mutuamente sobre a questão da segurança cibernética e, denúncias de invasão *hacker r*ealizada pela Rússia em sistemas de informáticos de empresas e prestadoras de serviços essenciais dos EUA.

Segundo Malcolm Moore, a *Munk Centre for International Studies* em Toronto/EUA, foi descoberta uma rede de espionagem que possuía capacidade eletrônica para deflagar a possibilidade de guerra cibernética contra os EUA. (MOORE, 2009)

Tal projeto espião foi denominado de Ghostnet[70] e representou:

> A descoberta do GhostNet que foi projetado para se infiltrar em ministérios e embaixadas sensíveis - e é conhecido por ter tido sucesso em muitos casos [...] O estudo revelou que quase um terço dos alvos infectados pelo GhostNet são 'considerados de alto valor e incluem computadores localizados em ministérios de relações exteriores, embaixadas, organizações internacionais, mídia de notícias e ONGs'. Essa rede global de espionagem foi construída nos últimos dois anos. [...] um relatório do Pentágono, divulgado na semana passada, disse que o exército chinês 'frequentemente cita a necessidade da guerra moderna de controlar a informação, às vezes chamada de 'domínio da informação'.
>
> No 10º Congresso Nacional do Povo, em 2003, o exército chinês anunciou a criação de 'unidades de guerra de informação'. O general Dai Qingmin disse que os ataques pela Internet ocorreriam antes de qualquer operação militar para paralisar os inimigos. (MOORE, 2009)

Tal realidade leva a presumir que a guerra cibernética já era uma possibilidade latente antes do conflito entre a Rússia e Ucrânia, posto que as nações com domínio econômico no mundo, já estavam criando estruturas para adaptar-se para ao novo modelo de conflito do século XXI, criando expertise e domínio das ferramentas e métodos de dominação através de meios digitais.

Não obstante, haver tensões envolvendo Estados Unidos da América, China, Irã e Rússia, a efetivação do que pode ser considerado como *guerra cibernética* efetivamente ocorreu em fevereiro de 2022, através da guerra iniciada pela Rússia ao invadir sistemas e infraestruturas críticas de tecnologia de informação da Ucrânia, seguida da invasão bélica territorial surpreendendo o mundo ocidental neste início de século XXI.

A guerra iniciada pela Rússia[71] contra a Ucrânia e a tentativa de tomada do país vizinho, está em execução exatamente neste momento, tem sido justificada pelo país invasor, a

[70] Tradução livre: internet fantasma;

[71] A guerra entre a Rússia e a Ucrânia completa dez meses com mais de 3 milhões de pessoas obrigadas a se refugiarem em outros países e com mais de 240 mil mortos, segundo os EUA, apesar do governo da Rússia manter o discurso no país de que esta não é uma guerra, e sim, uma mera operação militar, não tendo declarado formalmente o *Estado de Guerra* contra aquele país invadido. Reportagem da BBC News Brasil. Disponível em https://www.bbc.com/portuguese/internacional-63582629. Acesso em 23 Nov. 2022.

Rússia, com o objetivo de combater os resquícios do nazismo naquele país, contudo, não havendo provas reais desta denúncia. Não obstante, a Constituição da Rússia adotada em 1993, determina que são supremos valores os *direitos e liberdades humanas*, sendo a obrigação Estatal reconhecer, respeitar e protegê-los perante os cidadãos.

Apesar da retórica Russa, as potências econômicas do ocidente (EUA, França, Alemanha, entre outros) estão a apoiar a Ucrânia, realizando forte isolamento e restrições econômicas ao invasor, assim, trazendo a tona grande discussão sobre os riscos das tecnologias de inteligência artificial, algorítimos e *big data*, para a soberania e, mais preocupante ainda do ponto de vista humanitário sobre o uso para guerra de dominação.

Segundo Parks e Duggan (2001), a Guerra Cibernética possui alguns princípios significativos que auxiliam ou reduzem a capacidade de ataque e defesa dos oponentes no espaço cibernético, gerando vantagens competitivas ou não.

Nesse sentido, os princípios da ciberguerra se desdobram da seguinte forma: no princípio do efeito cinético (há uma dinâmica na produção de efeitos diversos); princípio da mutalibilidade; princípio do disfarce (tentativa de assumir identidade da autoridade que acessa a informação); princípio da dualidade do armamento (PARKS; DUGGAN; 2001); mais de uma função como ataque e defesa.

Na mesma direção, tem-se o princípio da compartimentação (cada parte controla uma parte do ciberespaço); princípio da usurpação (tentativa de controlar o oponente); princípio da incerteza (o ciberespaço é naturalmente inconsistente e não confiável) e o principio da proximidade (não existe proximidade física no ciberespaço e é comum a extraterritorialidade nos ataques). (PARKS; DUGGAN; 2001)

Para minimizar as vulnerabilidades quanto à segurança da informação diversos países estão criando estrutura de segurança cibernética para fazer frente a possíveis riscos, como retrata Leite Silva (2014), o Brasil tem sido um destas nações e vem estabelecendo várias normativas e órgãos neste sentido, como a Política Cibernética de Defesa, a criação do Sistema Brasileiro de Defesa Cibernética (SBDC), visando fortalecer as estratégias do país para atuar no domínio cibernético.

No tocante aos riscos mais evidentes, tem-se o incremento da espionagem a partir dos recursos da inteligência artificial e das tecnologias de *big data* e algorítimos, podendo ter consequências como o desligamento de infraestruturas tecnológicas importantes dos países e cruzamento de dados para geolocalização de governantes *inimigos*, e golpes por deposição.

Na guerra cibernética, incidentes cibernéticos que vão além de uma ocorrência simples, mas que se fundamentam em uma cadeia de ataques e geração de vulnerabilidades,

estes podem atingir estruturas de tecnologia da informação e segurança de modo virtual, como ser direcionada a paralisação de serviços essenciais importantes do país atacado.

Ademais, equipamentos ligados ao fornecimento de serviços essenciais, em muito, encontram-se automatizados por programas de computação, logo, quando atacados, paralisam a produção prejudicando a população na aquisição de tais serviços, como distribuição da água, energia, produção de alimentos, podendo intervir, inclusive, em sistemas automatizados ligados a saúde e hospitais, com risco direto a vida humana.

Como relata Wendt (2011, p.4) a ação hacker dentro da lógica da ciberguerra, pode atingir as "*infraestruturas criticas de uma região e/ou país e redundar em resultados catastróficos e imensuráveis quando, v.g. provocar um colapso na rede de transmissão de energia, causando apagão e/ou retardando o retorno do serviço*"; afetando a soberania e segurança do país, de modo grave.

Nesse sentido, expõe Sampaio (2001), que são objetivos preferenciais da guerra cibernética os programas computacionais que gerenciam:

> 1. comando das redes de distribuição de energia elétrica; 2. comando das redes de distribuição de água potável; 3. Comando das redes de direção das estradas de ferro; 4. comando das redes de direção do tráfego aéreo; 5. comando das redes de informação de emergência (pronto-socorro, polícia e bombeiros). 6. comando das redes. bancárias, possibilitando a inabilitação das contas, ou seja, apagando o dinheiro registrado em nome dos cidadãos (o potencial para o caos e a desmoralização de um país embutido neste tipo de ataque é por demais evidente); 7. comando das redes de comunicações em geral, em particular (redes de estações de rádio e televisão); 8. comando dos "links" com sistemas de satélites artificiais (fornecedores de sistemas telefônicos,de sistemas de sinais para TV, de previsão de tempo, e de sistema GPS); 9. comandos das redes dos Ministérios da Defesa e, também do Banco Central e outros ministérios chave (Justiça, Interior etc);10. comandos dos sistemas de ordenamento e recuperação de dados nos sistemas judiciais, incluindo os de justiça eleitoral. (SAMPAIO, 2001)

Tal realidade ficou notória durante o pioneiro registro de guerra cibernética entre a Rússia e a Ucrânia, que concentraram batalhões de hackers[72] que trabalharam quebrando a segurança cibernética dos países opositores e atacaram, ciberneticamente e mutuamente, retirando o acesso a sites e provedores de internet.

[72] Hackers, indivíduos especializados em ciência da informática especializados em vulnerabilizar a segurança da rede de computadores, se uniram em locais geograficamente distintos do mundo, para apoiar a Ucrânia e atacar infraestruturas informáticas da Rússia após esta ter invadido o território ucraniano em fevereiro 2022.

Nesta experiência da guerra entre a Ucrânia e a Rússia ficou evidente ataques de ambos os lados, nas quais as táticas giraram em torno da obstrução do compartilhamento de informações, intervindo na transmissão de informações intraguerra, com significativa retirada de operação de serviços diversos essenciais, deixando notório a desigualdade de armas do ponto de vista do desenvolvimento tecnológico.

Como retratou o CEO da Ukrtelecom da Ucrânia, em ataque que reduziu em 13%, o trafego do maior provedor de internet daquele país:

> um poderoso ataque cibernético inimigo foi realizado na infraestrutura de TI da Ukrtelecom. Para proteger a infraestrutura de rede crítica e não interromper os serviços às Forças Armadas, outros órgãos militares e usuários de infraestrutura crítica, fomos forçados a restringir temporariamente o acesso à Internet à maioria dos usuários privados e clientes empresariais. (CISO ADVISOR, 2022a)

Por outro lado, atingindo infraestruturas tecnológicas de informática da Rússia, a NetBlocks que realiza a tarefa de monitora a conectividade global na internet, informou que pode observar um esquadrão de hackers[73] espalhados pelo mundo conseguiram interromper serviços de internet russo e que sites importantes como do Kremlin e da Duma (câmara do parlamento) ficaram inacessíveis, bem como, foram interrompidos serviços do governo ligados à mídia apoiados pelo Estado, energia entre outros. (CISO ADVISOR, 2022a)

Ademais, a discussão sobre o conceito de guerra cibernética supramencionada subexiste, de modo não pacífico, justamente em razão de estudiosos defenderem que os resultados dessa guerra digital não devem ser comparados aos resultados de uma guerra bélica comum, haja vista, as mortes e a subjugação da população, que podem ocorrer.

Contudo, é importante ampliar a visão para os riscos dessa modalidade de guerra com o incremento da inteligência artificial e sobre os caminhos que podem ser redesenhados pelo direito diante de nações em guerra, sendo necessário cobrar a paridade de armas diante das novas tecnologias.

---

[73] Em entrevista realizada pelo jornal *The Guardian (EUA),* o Presidente da Netblocks informou que mais de *300 mil hackers* se disponibilizaram a combater a Rússia em defesa da Ucrânia, formando um grupo na rede social Telegram chamado de *Tropas Ucranianas de TI;* após convite do Ministro da Transformação Digital da Ucrânia, Mykhailo Fedorov que enviou um link de participação, visando criar guerreiros de tecnologia da informação em meio a guerra cibernética. (CISO ADVISOR, 2022a)

Essa guerra cibernética se apresenta como uma modalidade cuja consequência ainda não é possível conhecer os resultados; a carência dessa experiência em guerras e a observação do conflito entre a Rússia e Ucrânia, demonstram que estas tentam desestabilizar as estruturas de controle e tecnologias da informação, mutuamente, contudo, não se sabe o alcance que esta realidade poderá alcançar.

O que se tem de forma bem clara é que, a igualdade de armas, é uma das garantias que os sistemas de inteligência artificial devem promover no plano regulatório, segundo a Comissão Europeia para a eficácia da justiça (CEPEJ, 2018); sendo necessário, a *paridade de armas*, para que meios tecnológicos não causem desequilíbrios, favorecendo alguns operadores e colocando dificuldades a outras populações, na batalha geopolítica.

4.2.11 Risco de guerras com armas tecnológicas de longa distância

Existe atualmente uma tensão global no ocidente sobre a disposição de equipamentos tecnológicos de última geração para o âmbito das guerras, em especial, após o advento da guerra entre a Rússia e a Ucrânia, país do leste europeu, cuja guerra *não declarada*, ocorre desde fevereiro de 2022, fato que tem apresentado uma nova dinâmica *perigosa* ao ambiente de guerra, em razão de tais armas poderem ser operadas à longa distância e com alto potencial destrutivo.

A ocorrência do lançamento de milhares de drones monitorados remotamente com bombas pela Rússia[74], recentemente lançadas contra a Ucrânia, se constitui um novo estágio de *dronificação da guerra* preocupante, especialmente como nos revela Filippo Ruschi (2022), por estar ocorrendo fora dos limites territoriais do conflito em solo, fato que demonstra a violação de normas internacionais sobre guerras, fragilizando-as diante do desenvolvimento e emprego de novos instrumentos tecnológicos.

Não obstante a utilização desses drones com câmeras de alta resolução, o maior ponto de preocupação da comunidade internacional nesse momento, ocorre em razão da ameaça do governo da Rússia (Vladmir Putin), de empregar mísseis com geolocalizador de alta precisão com ogivas nucleares direcionadas contra os países do continente europeu, caso continuem dando suporte bélico a Ucrânia; assim, tal ameaça gerou alerta em nível máximo, diante do risco dessa tecnologia ser efetivamente operada contra o mundo ocidental.

[74] Veja mais em https://www.bbc.com/portuguese/internacional-62291582. 25 Jul. 2022

Reforça-se neste trabalho acadêmico, que tais os riscos advindos dessas tecnologias já se encontram atualmente unidos às técnicas de inteligência artificial, algorítimos e sensores de geolocalização, que trazem uma nova e potencial possibilidade de destruição em massa, mesmo em espaços físicos não militarizados, ferindo normas internacionais, mas também, uma ética mínima de guerra a partir da vulnerabilização da população comum, não envolvida diretamente no conflito.

Compreender um pouco mais sobre essa dinâmica, com visão meramente introdutória, se faz necessário para melhor compreender os riscos da inteligência artificial na potencialização dos equipamentos tecnológicos utilizados à distância no âmbito das guerras, ademais, por não ser um risco apenas localizado e sim, que pode alcançar um risco efetivamente existencial, em última análise, como veremos a seguir.

a) Risco de Dronificação da Guerra

Como retrata Grégoire Chamayou (2015), na sua teoria do drone[75], os Estados em guerra utilizam da relação entre *conhecimento e força violenta* para gerar uma hegemonia na batalha, os drones nessa relação *são "[...] câmeras de vídeo voadoras, de alta resolução, armadas de mísseis".*

Os drones são equipamentos considerados pelos cientistas como elemento de uma terceira revolução de armas bélicas, posterior a pólvora e as armas atômicas, a partir do incremento da inteligência artificial, tecnologia lhes confere automação decisória, atuando sem a necessidade da intervenção humana.

Possui duas características principais: a possibilidade de *tudo filmar* e a capacidade de *projetar força de modo remoto*; assim, possui a autonomia da vigilância e pode materializar poder sobre um objeto, sem a necessidade da ação humana embarcada ou no local de ataque (CHAMAYOU, 2015); características importantes na análise do seu uso como instrumento de guerra e diante dos direitos fundamentais à proteção de dados e à privacidade.

Nessa dinâmica, a autonomia de vigilância apresenta o risco inicial quanto a proteção de dados, em razão do poder de identificação e controle da vida das pessoas, que segundo Chamayou (2015), começa com a coleta de dados sensíveis, arquivamento e indexação de informações do sistema de vigilância e a posterior produção cognitiva autônoma da máquina, cruzando dados e promovendo uma cartografia da vida das pessoas.

[75] Livro Traduzido por Célia Euvaldo. São Paulo: Cosac Naify, 2015.

Os drones foram criados por John W. Clark em 1965, com o intuito de serem utilizados em ambientes hostis, *de modo a evitar* a vulnerabilidade do homem no conflito, para que estivesse mais protegido ao comandá-lo a partir de um local cujo corpo biológico estivesse seguro, logo, manipulando-o à distancia. (CHAMAYOU, 2015)

Na escala evolutiva, os drones tornaram-se mais avançados durante a segunda guerra mundial e foram denominados de "*drones-alvo*" pelo exército norte americano, descontinuado em 1970, mas retornado à produção, após o ataque de 11 de setembro de 2001 nos EUA, quando passou a ter mísseis anticarro. (CHAMAYOU, 2020; p.242)

A guerra que tradicionalmente ocorreria de modo equilibrado quanto ao emprego dos homens no terreno desconhecido, pelo manejo de material bélico e da logística, transforma-se em uma *guerra unilateral*, antiética e destruidora, estendendo-se a espaços não-militarizados, fora do ambiente do próprio do conflito.

Atualmente teve ainda, o incremento de sensores, aparelhos de geolocalização e recursos de IA que potencializam suas *capacidades humanas*, com poder de vigilância e captação de imagens, que lhes dão certo grau de *onisciência.* (RUSCHI, 2022)

No âmbito da guerra, os drones são preocupantes em razão dos riscos quanto à superioridade tecnológica que uma nação desenvolvida pode ter em relação à outra; como consta nos relatórios oficiais[76], na atual guerra da Ucrânia com a Rússia, por exemplo, a nação violada detinha apenas 50 drones fabricados na Turquia, enquanto a Rússia, nação que empreendeu a campanha conflituosa, detinha milhares desse equipamento.

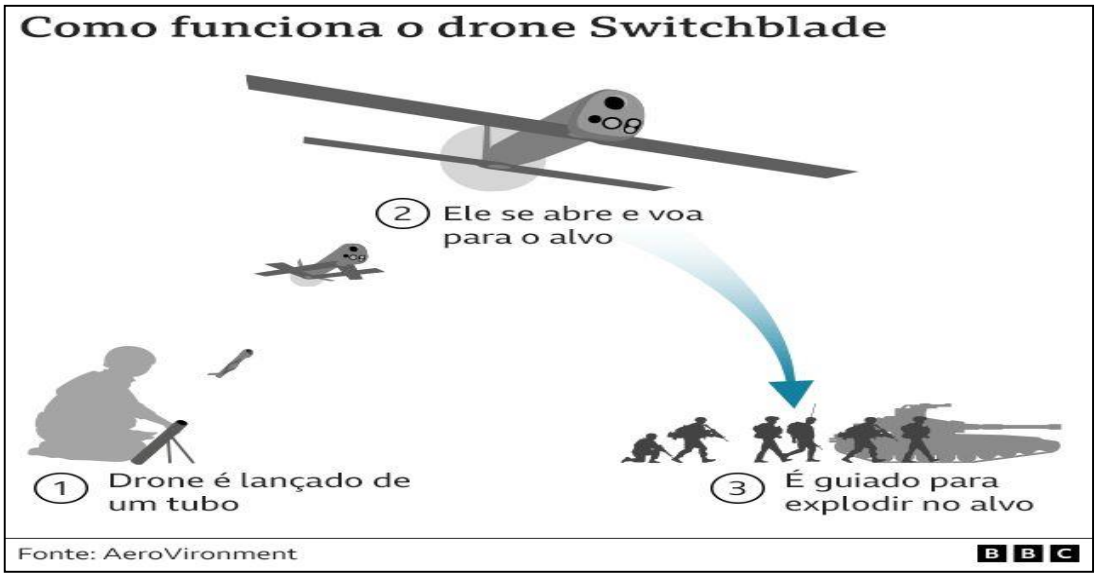
A *guerra unilateral* como retratou Chamayou (2015, p.195) apresenta o drone como um instrumento de homicídio "*fora de combate*", que entretanto, possui o poder de alterar as relações do conflito, entre combatentes de modo desigual e entre sociedade e Estado, este por sua vez, responsável em proteger seus súditos e retomar o estado de paz, sendo este o suposto objetivo da guerra.

Note que nessa teoria do drone o Chamayou (2015), reflete que a dronificação da guerra é uma arma humanitária capaz de reduzir a vulnerabilidade dos combatentes, sendo supostamente direcionada a poupar suas vidas, ao contrário, do que a norma apresenta, cuja proteção deve focar nas pessoas civis.

[76] *"Milhares de drones estão sendo usados na guerra da Ucrânia - para detectar posições do inimigo, lançar mísseis e fogo direto de artilharia*". CNN (2022, p.1). Alguns modelos de drones voam a mais de 180 km/h e alcançam mais de 2.000 quilômetros de distância, podem ter pequenas cargas explosivas ou mísseis poderosos. Os drones denominados "kamikaze" possuem explosivos e são lançados em um tubo propulsor e após a eclosão, são direcionados ao alvo, portanto, alcançam grandes distâncias.

Na perspectiva de Chamayou (2015, p.197), o Estado transfere a proteção do indivíduo que estaria na guerra para a coletividade ao usar o drone de ataque à distância, fato que no século XXI, tornou-se mais evoluído com os telecomandados, permitindo maior distanciamento do local de ataque.

IMAGEM 2
FUNCIONAMENTO DOS DRONES *"KAMIKAZE" (SWITCHBLADE)*



Fonte: BBC News Brasil, 2022. (reprodução)

Não obstante o lapso temporal da obra, e a atual realidade da guerra Rússia-Ucrânia, cuja realidade fática tem apresentado novos desafios ao mundo ocidental; há uma enorme vulnerabilidade dos combatentes de guerra no terreno e incremento da violência contra a coletividade civil da nação agredida, mesmo fora dos territórios do conflito, tornando preocupante o uso dos drones nesta guerra. (RUSCHI, 2022)

O drones enquanto instrumento de guerra unilateral, desequilibra a equivalência de forças entre combatentes, sem a reciprocidade intersubjetiva da guerra tradicional, não reduz vulnerabilidades para a sociedade civil e amplia os riscos de sofrerem violência de modo deletério, tornando-se instrumento desigual.

A dronificação da guerra potencializada pela automação produzida pela inteligência artificial e recursos de geolocalização, tem produzido ataque e morte à longa distância, atingindo espaços dentro e fora dos territórios definidos na campanha de guerra,

sendo terrivelmente deletério e sem critérios de segurança mínimos para proteção da população civil, face o uso indiscriminado deste recurso.

Unido ao monitoramento e captação de dados por meio de imagens continuas e não contínuas, os drones estão se tornando uma forma deletéria de atingir o inimigo, na maioria das vezes, sob o desejo de poder e dominação hegemônica, enquanto as normativas internacionais e os princípios éticos e humanitários vão se deteriorando diante da operacionalização desse instrumento de guerra, que se apresenta cada vez mais evoluído e mais nocivo. (RUSCHI, 2022)

b) Risco de ataque nuclear à distância

O nível de tecnologia que os mísseis hipersônicos da Rússia apresentam são avançados e as ameaças realizadas contra os países apoiadores da Ucrânia, que reagiram à fragilização da soberania desta, durante a invasão, tornam-se elementos de preocupação global, com a escalada deste conflito.

O presidente da Rússia como meio de persuadir os chefes de Estado dos países ocidentais como Paris, Berlin e Londres, bem como, das nações fronteiriças como a Finlândia e Suécia, passou a realizar ameaças e deixou a humanidade em alerta sobre possibilidade de utilização de armamentos nucleares no conflito.

Deste modo, há um elemento de destaque importante nesse modelo de guerra, que consiste na utilização de instrumentos bélicos à longa distância, de modo extraterritorial, diferente das guerras do século XX, que eram travadas em espaços territoriais específicos.

Tal possibilidade de guerra nuclear a partir de tecnologias da informação e inteligência artificial permitem que não sejam empregadas estruturas logísticas presenciais ou que demandem de efetivo e soldados *in loco*, no local que se deseja dominar ou atingir, o que torna um possível ataque menos custoso e que pode ser disparada à longas distâncias, além de gerenciadas sua trajetória e alvo.

Na concepção de Boyd (2022) engenheiro aeroespacial que estuda os sistemas de defesa, espacial e hipersônico, professor de engenharia aeroespacial da Universidade do Colorado nos EUA, retrata que o desenvolvimento pela Rússia, China e EUA dessa tipologia de míssel, tem como risco maior, a dificuldade de se defenderem de possíveis ataques devido à velocidade, manobrabilidade e trajetória de voo que esses hipersônicos podem alcançar.

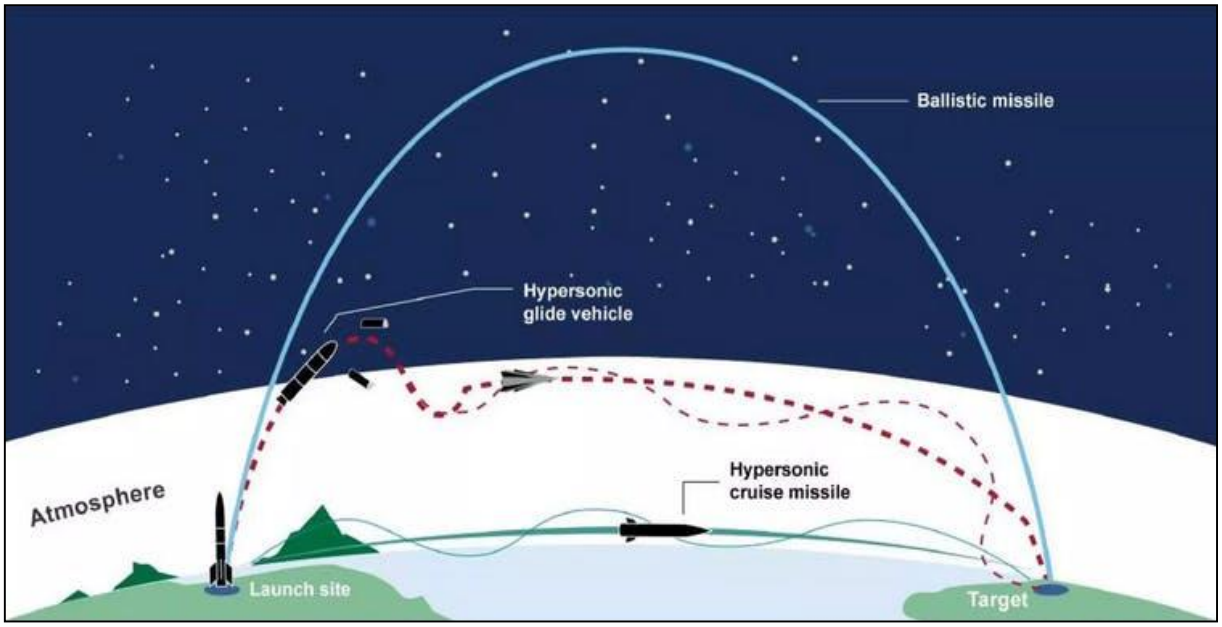
Apesar das tecnologias sobre mísseis existirem desde 1962, e os hipersônicos em 1980, a atuais tecnologias de georreferenciamento, inteligência artificial e novos padrões de

propulsão, elevaram a capacidade dos mísseis de terem suas trajetórias modificadas enquanto viajam, representando uma ameaça significativa à segurança nacional e global. (BOYD, 2022)

Países sem as mesmas tecnologias podem se tornar presas fáceis dessa faceta tecnológica artificialmente concebida, que atua de modo muito veloz e tem alto potencial destrutivo e à distância, elemento importante na análise.

Um dos grandes riscos é o que decorre do míssel hipersônico operar na atmosfera em região mais alta que as outras armas comumente utilizadas, e apesar de voarem mais baixo que os mísseis intercontinentais balísticos, há uma dificuldade de rastreamento além da facilidade de modificação de trajeto durante a viagem.

IMAGEM 3
TIPOS DE MÍSSEIS HIPERSÔNICOS E COMO TRAFEGAM NA ATMOSFERA



Fonte: Escritório de Contabilidade do Governo – EUA (BOYD, 2022)

A imagem 3, demonstra três tipos de mísseis hipersônicos, sendo o veículo hipersônico da nova geração tecnológica (*hipersonic glide vehicle*), atua em alta velocidade e em média altitude atmosférica, com um sistema planador que permite excepcional manobrabilidade, que permite ter seu alvo modificado durante a trajetória, além da vantagem quanto à dificuldade de seu rastreamento.

A velocidade deste míssel é muito superior ao de cruzeiro, da geração anterior, que opera em baixa altitude e é fácil de ser rastreado, (*hypersonic cruise missile*), mas possui

velocidade menor que o veículo balístico intercontinental (*ballistic missile*), que opera em altitudes ainda maiores, mas possui maior custo de produção para larga escala.

Para melhor compreensão, um míssel desta nova geração tecnológica, possui velocidade muito superior a do som, que equivale a 1.225 quilômetros por hora (km/h) no nível do mar ou a 1.067 km/h a mais de 10 mil metros de altitude. (BOYD, 2022).

Os voos dos jatos comerciais de passageiros atingem uma velocidade inferior a 966 km/h, enquanto os mísseis hipersônicos operam a velocidade de 5.633 km/h, cerca de 1,6 km por segundo, seis vezes mais. (BOYD, 2022)

Note que mesmo os EUA, países aliados europeus, Rússia e mesmo a China, nações consideradas mais avançadas neste tipo de tecnologia, ainda não possuem nessa região intermediária atmosférica, grandes capacidades de rastreamento de mísseis hipersônicos, tornando-se tecnologia que é razoável o risco de não conseguir detê-lo em caso de ataque.

Outro elemento de risco perturbador e global, é a ameaça da Rússia em operar tais mísseis com ogivas nucleares em detrimento do armamento bélico tradicional; o que levaria uma possível nação inimiga em caso de ataque, a decidir sobre a probabilidade desse armamento ser nuclear ou convencional (BOYD, 2022).

É de bom alvitre refletir, que mesmo as respostas preventivas dos países ameaçados também seria deveras preocupante, devido à iminência de desencadear uma guerra nuclear mundial e generalizada, de proporções e resultados inimagináveis e nos quais os países mais vulneráveis seriam aqueles cujas tecnologias ainda estão se construindo.

Fato é que tanto na guerra cibernética quanto o uso de armas nucleares com alto poder de destruição em massa, podem nesse momento histórico ser operadas à longa distância, com base nas tecnologias de IA e automação, que podem comprometer a vida tornado-se um risco ainda maior que a guerra tradicional, cujas características se diferem das atuais estratégias de guerra.

Como já ressaltado anteriormente na guerra tradicional, muitos elementos contribuem para o sucesso de uma nação em detrimento da outra, a exemplo, da disposição da tropa, tempo, clima, capacidades de gestão de recursos logísticos e de alimentação que geram limitações naturais, com riscos a ambas as partes.

Os mísseis hipersônicos, diferentemente, possuem alto nível de automação, sistemas de georreferenciamento e propulsão, que permitem mais velocidade e alta precisão em relação ao alvo, realizam rápida viagem atmosférica, podendo ter sua trajetória modificada com

excepcional manobrabilidade, além da probabilidade de conter ogivas nucleares[77], o que torna tal instrumento de guerra desastroso, diante das tensões geopolíticas deste momento.

Nessa mesma direção, enquanto produzimos esta pesquisa acadêmica a humanidade acompanha atônita e preocupada, as informações relativas às ameaças da Rússia contra países europeus por apoiarem a defesa da soberania da Ucrânia.

Conforme a agência de notícias da Itália, *Corriere della Sierra* (2022), as ameaças da Rússia contra o países da união europeia permanecem a ocorrer de modo público, ao revelar que a TV estatal russa divulgou uma simulação em vídeo, na qual mísseis hipersônicos levariam pouco tempo para atingir o alvo, caso fossem disparados da base de Kaliningrad, contra países europeus.

IMAGEM 4
SIMULAÇÃO DE TEMPO PARA MÍSSEL RUSSO ATINGIR A EUROPA

Fonte: Jornal Corriere della Sierra (22 abr. 2022)

A simulação retratou a possibilidade de um míssel hipersônico atingir Berlin (Alemanha) em apenas 105 segundos, alcançar Paris (França) em 200 segundos e Londres (Inglaterra) em 202 segundos, reforçando, a possibilidade de lançar por submarino, mais de 50 mísseis nucleares que poderiam destruir os EUA. (CORRIERE della Sierra, 2022)

[77] O presidente Vladimir Putin, presidente da República Russa realizou apresentação na mídia daquele país, sobre a capacidade temporal dos mísseis hipersônicos, informando serem capazes de transportar uma ogiva nuclear e alcançar países da Europa, em mínimo espaço de tempo; este fato gerou enorme preocupação da União Europeia e da ONU sobre as ameaças nucleares daquele governante para o mundo.

Tal ameaça grave, em se realizando poderia comprometer todo o mundo pelas consequências desastrosas que acarretaria em cadeia em relação a outras nações e o envolvimento de entidades de proteção internacional, além da fragilização do direito humanitário, em razão da quebra da soberania de Estados e de vulnerabilização de democracias, constituindo-se enorme risco humanitário e global de grau elevadíssimo.

A imagem acima representa uma reprodução do jornal italiano, sobre a simulação gráfica (hipotética) com a trajetória de mísseis nucleares divulgada pela Televisão estatal Russa, após o discurso do Presidente Vladmir Putin dizer que o país possui mísseis supersônicos capazes de superar todos os sistemas de defesa do mundo, ameaça agressiva que deixou analistas ocidentais em alerta sobre a hipótese de ataque nuclear a capitais europeias. (CORRIERE della Sierra, 2022)

Tais riscos demonstram que as maravilhas que as tecnologias estão trazendo para a vida em sociedade, não podem ser afastadas do poder de observação da sociedade sobre seus efeitos e utilização nociva para crimes ou para fins de guerra, fragilizando soberanias.

Por um lado, as guerras ainda possuem um pensamento atrelado ao modelo imperialista do século passado, mas empregam na atualidade, instrumentos tecnológicos sofisticados que podem levar o restrito conflito de uma guerra localizada, a uma grave ameaça e consequente afetação da humanidade, a partir de *um mero botão.*

É importante, que a atual sociedade tenha a compreensão de que o direito pátrio e internacional constituído desde a segunda guerra mundial, precisa ser revisitado e repensado, para limitar que as tecnologias de inteligência artificial, sejam utilizadas para a guerra, e para projetos de poder geopolítico, ferindo de sobremodo a paz social e a dignidade humana.

5. PILARES ÉTICOS, ANTIDISCRIMINATÓRIOS E HUMANITÁRIOS PARA O DIREITO.

> *"O direito, contudo, como conceito teleológico, arrojado ao meio da engrenagem caótica dos objetivos, aspirações, interesses humanos, é constrangido constantemente a tatear na busca de seu caminho e, uma vez o haja encontrado, tem que derrubar obstáculos presentes..."*
>
> Rudolf Von Ihering (2019, p.30)

O Direito quando bem direcionado possui grande importância como ferramenta de liberdade e promoção da igualdade social, corroborando com o processo de convivência

pacífica entre os povos e manutenção da espécie humana no plano social, a partir da capacidade de impor limites e regular as relações de poder existentes, constituindo-se, portanto, um ímpar instrumento de luta da sociedade.

A discussão sobre a necessidade de fundamentar esse Direito nos pilares expostos nesse trabalho, não se encontra na além da promoção do conhecimento científico, na capacidade de fomentar no interior de cada pessoa, *"uma força suprema, ou seja, aquela sólida e corajosa"* pautada no "*sentimento do direito",* como refletiu Ihering (2019, p.13), capazes de direcionar as decisões mais importantes para o bem estar social, ainda que, subsistam lacunas fáticas a superar.

Acredita-se que alguns pressupostos éticos, possam combater a discriminação racial e social, além de resultar na proteção da humanidade das pessoas, se bem tutelados pelo Direito, agora com iniciativa temporal ante e pós, em razão da dinâmica das transformações sociais, adaptando-se e se renovando, na implementação de instrumentos de proteção.

Há, contudo, no atual contexto advindo da inovação tecnológica deste início de século XXI, a discussão de que o Direito tem sido ineficaz nessa temática tendo caminhado para a obsolência e a crise, ao demonstrar uma lacuna no ordenamento jurídico para gerir tal temática da inteligência artificial no âmbito social, além destas no ambiente de guerra, por tudo, vulnerabilizando a plena proteção dos direitos humanos e fundamentais da sociedade.

As tecnologias desta nova indústria 4.0, inteligência artificial, uso de algorítimos para processos decisórios (imprecisos) e *big data* (com caráter discriminatório) ou mesmo utilização de dados para condições de guerra e poder geopolítico, possuem um caráter perigoso, com risco autofágico, da própria sociedade, dependendo de uma nova regulação, atualizada para os tempos atuais.

Nesse contexto, repensar e propor novos pilares para o Direito deste início de século, diante das novas tecnologias da inteligência artificial, apresenta-se como desafio jusfundamental desta geração, que em última instância desemboca na proteção dos direitos humanos e fundamentais, e mesmo da humanidade, em sua máxima expressão.

Não há aqui, qualquer defesa de um viés puramente positivista da norma, mas, a defesa de uma concepção que vai além, pautada na hermenêutica e interpretação que se baseie nos valores fundamentais da sociedade e que considere o valor axiológico e amplo da norma constitucional, quando estabelece o conteúdo da proteção de dados sensíveis.

Portanto, a análise dos três pilares jusfundamentais para a reconstrução do direito, expostos nesta pesquisa, fundamentam-se principalmente, na legitimidade da norma perante a sociedade, no âmbito que vai além do direito positivado, tendo por si só um viés *supraposítivo*

que emerge da vontade popular em busca da significativa dignidade da pessoa humana, como princípio *prima facie* a ser alcançado nas relações sociais, na qual deve se pautar o uso das tecnologias.

Não obstante, considerando que as novas tecnologias têm apresentado novos instrumentos de decisão, e também, de guerra, é urgente estabelecer um novo *contrato social*[78] que seja capaz de frenar e regular iniciativas tecnológicas prejudiciais à proteção dos indivíduos em sua singularidade humana, além das suas liberdades públicas, quando não afetam a vida efetivamente.

Para tanto, reestruturar o direito sob os pilares éticos, na postura de antidiscriminação e com vistas à proteção dos atributos de humanidade das pessoas, portanto, com caráter humanitário do direito, torna-se imprescindível para evitar a expansão de estruturas autofágicas que se desenvolvem no processo de desenvolvimento tecnológico.

Seja por desconhecimento ou por ambição exacerbada, mas que possuem alto potencial nocivo com capacidade de desencadear estruturas destrutivas coletivas, que precisam ser mensuradas e melhor reguladas pelo ordenamento jurídico; há a necessidade de atualização e reconstrução do Direito para atender as dinâmicas do século XXI, em especial, diante da velocidade e expansão da inteligência artificial, como instrumento de poder.

5.1 PILAR ÉTICO PARA O DIREITO

A discussão sobre o pilar ético no direito torna-se cada vez mais importante diante dos avanços das tecnologias digitais, em especial, diante do emprego dos algorítimos matemáticos para o processo decisório de *máquinas inteligentes* e dos recursos resultantes das inovações computacionais, cujas tarefas orbitam no âmbito digital, estas denominadas, de modo *lato sensu,* de inteligência artificial, catalisando o uso dos dados pessoais como objeto de valor econômico, político, ideológico, ou mesmo, geopolítico e entre Estados.

Diante da superconectividade digital, a interação do homem com tais máquinas inteligentes fora ampliada de sobremodo retroalimentando a *smartificação* das tarefas e da vida,

[78] Jean Jacques Rousseau defende a realização de um contrato entre seres sociais, que permita preservar a liberdade individual do homem, ao mesmo tempo em que é garantido a segurança e o bem-estar da vida em sociedade, na qual a soberania da sociedade e a vontade política coletiva prevaleceria sobre as intenções individuais, conformando as relações. V. ROUSSEAU, J.J. Do contrato social. (tradução de Lourdes Santos Machado), 2ª edição-São Paulo: Abril Cultural, 1978. (Os Pensadores).

exponencialmente, ampliando os riscos pelo uso indiscriminado dessas tecnologias preditivas, pela carência regulatória no campo ético, em especial, no Brasil.

A possibilidade de ter mitigado o exercício de direitos fundamentais, comprometendo o princípio da autonomia e do livre consentimento das pessoas no uso dos recursos digitais, da proteção da privacidade, e até em última instância, ser da utilização de tais tecnologias como instrumento de guerra e conflitos geopolíticos capazes de sucumbir a vida humana, demonstram os prejuízos ao exercício da cidadania, das liberdades públicas e da proteção da vida, que podem tornar-se incomensuráveis.

Na visão de Bostrom e Yudkowsky (2011; 202), a inteligência artificial tem desempenhado um papel cada vez mais amplo na sociedade e se tornará, possivelmente, ainda mais importante no futuro, portanto desenvolver algorítimos de IA que não sejam apenas "*poderosos e escaláveis*", mas também "*transparentes"* para serem monitorados.

Torna-se fundamental, tal concepção, quando o algorítmo de IA sai do aspecto meramente técnico matemático ou robótico para o âmbito cognitivo das esferas sociais, ou seja, quando passam a desenvolver tarefas cognitivas que antes eram inerentes aos seres humanos, herdam, portanto, as mesmas exigências sociais cobradas pela sociedade. (BOSTROM; YUDKOWSKY, 2011)

Contudo, o Direito brasileiro apresenta certa obsolência diante dessa nova dinâmica social e mesmo no mundo, há um movimento ainda incipiente para a construção de marcos regulatórios nessa temática.

Assim, é necessário avançar para regular a criação e a aplicação das diversas tecnologias de inteligência artificial, que já estão, nesse mesmo momento de análise, sendo já utilizadas, por vezes de forma abusiva pela falta de regras transparentes, comprometendo e suplantando muitos pontos positivos e benéficos que estes avanços apresentam no escopo do desenvolvimento social.

Diante de tais riscos, implementar uma nova mentalidade filosófica é necessária, que se paute no aspecto ético do direito e possa concebê-lo sob novos vieses voltados a realidade da inovação tecnológica, com cuidado e clareza.

Como retrata Adeodato (2021), se faz necessário a implementação de atualizada filosofia do direito para fomento de uma nova ética no ordenamento jurídico, contudo, importante conceber que este ciclo não é fácil de ser transmutado, posto que o estabelecimento de novos modelos de pensar, as ideologias anteriores permanecem no ambiente modificado.

A concepção sobre uma nova filosofia do direito, propondo uma nova ideia ou ética para o ambiente social, além de não ter o condão de substituir o pensamento anterior existente,

permanece lá em paralelo com a nova filosofia, fazendo parte de um aglomerado filosófico cultural, como por exemplo, ocorrido na cultura da Europa, que absorveu as contribuições do Judaísmo, do Cristianismo, da Grécia e Roma antiga. (ADEODATO, 2021).

Deste modo, haverá sempre um mesclado de concepções filosóficas latentes, antigas e novas, que irão interagir e precisam ser enxergadas, administradas e selecionadas nessa dinâmica, e por vezes, combatidas, quando as históricas concepções não mais atendem aos valores axiológicos da sociedade, ademais, quando busca-se alcançar a igualdade social.

De modo mais específico, tratando do *pilar jusfundamental ético do direito*, apesar das diferenças semânticas entre ética, moral, justiça e direito no pensamento ocidental, discussão historicamente inaugurada pelos filosóficos gregos socráticos, passou-se a existir como principal problema ético da filosofia do direito, a exigência de diferenciar o bom, do mau direito, contudo, a resposta não parece ser tão evidente, devendo ser racionalizado por diversos fatores. (ADEODATO, 2021).

Como discute Bostrom e Yudkowsky (2011), a possibilidade de construir sistemas de *inteligência artificial amigável* ou mesmo mau, direcionam no sentido de que o projeto maior dessa tecnologia é o de replicar o espaço da mente humana, e que esta premissa depende do desenho de IA que se está discutindo, além de outras variáveis, *sui generis*.

Tal questionamento possui total dependência da resposta sobre a capacidade de controle da programação de IA inicialmente realizada, se esta pode ser refletida nos efeitos futuros do sistema no mundo ou se o sistema de IA é impossível de controle total.

A capacidade que a *máquina inteligente* tem de acessar seu próprio código-fonte, recombinar e reescrever a si própria de modo autônomo, indicam que há impossibilidade de controle total e adequada da IA, posto a possibilidade da máquina transformar-se em qualquer coisa que deseje ser, isto significa resultar em uma *IA hostil* ou mesmo *IA Amigável*, contudo, não há atualmente, segurança sobre tal resultado. (BOSTROM; YUDKOWSKY, 2011; p.221)

O grande desafio ético atual é construir um sistema de IA que possa por si próprio torna-se cada vez mais ético, produzindo uma espécie de *boa ética* ou *superética,* a partir da mesma inteligência de máquina (BOSTROM e YUDKOWSKY, 2011; p.223).

Entretanto, não há capacidade técnico-científica, no momento atual para essa resposta, assim, os sistemas de IA encontram-se dependentes da autorregulação privada, da imposição de códigos e normas pelos entes estatais ou mesmo das pressões da sociedade civil.

Deste modo, conhecer sobre a ética (gênero) e a moral (espécie) envolvidas na temática das tecnologias, constitui-se instrumento de poder à população, no processo de compreensão da correlação entre estas e como podem ser empregadas como remédio preventivo

e repressivo para coibir abusos; contribuindo, portanto, no conteúdo valorativo que visa frenar excessos no âmbito dessas aplicações no plano real.

No escopo do direito sob o pilar ético, este é concebido a partir da idealização dos valores axiológicos *suprapositivos* construídos com base nos direitos humanos e fundamentais da sociedade, de modo legítimo do clamor do povo, ao mesmo tempo em que, fomenta a construção de normas prescritivas e analíticas para conceber no mundo real, meios adequados de tutela social, nesse viés, tentando frenar os riscos advindos do âmbito da inovação digital.

A ética traz, portanto, o objeto do elemento *moral*, precisamente, uma moral voltada para o bem estar social diante das novas tecnologias, cujo *"termo ética pode ser utilizado como conhecimento empírico dos meios e fins que os seres humanos empregam em sua vida comum, ou como o estudo das formas de controle estratégico desses meios e fins"*. (ADEODATO, 2021, p. 345).

Sob esta concepção, expõe Adeodato (2021), que a ética idealista e normativa se propõe a prescrever concepções no mundo fático a partir de um conjunto de valores ideais e com fundamentos lógicos, a serem internalizados pelos seres humanos e usados no plano real, assim, adequando a sociedade aos valores ideais de convivência.

Nessa direção, a discussão jusfilosófica ética *idealista e normativa* (ADEODATO, 2021), surge como proposta para a discussão sobre as novas tecnologias no cenário atual, ao se pautar no *dever-ser*, idealista, mas que se apresenta também de modo prescritivo, analítico e normativo, pautado no modelo axiológico que se fundamenta na consideração dos valores sensíveis da sociedade.

Tais concepções emergem do fato específico que este século XXI tem trazido como desafio social, o *paradigma jusfundamental da proteção de dados sensíveis*, como retrata Silveira (2022), sendo o principal paradigma do direito na atualidade.

Haja vista, a necessidade de tutela e justiça identitária dos indivíduos a apartir de seus dados sensíveis, cuja quebra, pode levar a falência o projeto do humanismo, pensado na reformulação do ordenamento jurídico no pós-guerra de 1945, e que culminou com a formação da ONU e suas normativas a partir de 1948.

Ocorre que com a utilização maciça das tecnologias da informação no estágio em que se encontram, como a robótica, indústria 4.0, inteligência artificial, algorítimos e o processamento de grande quantidade de dados da população (Big Data), tem suprimido a singularidade das pessoas, sendo estas resumidas a padrões de dados, utilizados de forma predatória por entidades privadas e públicas.

A autonomia de máquina se depara como as perspectivas do *constitucionalismo digital,* ou ainda, do *neoconstitucionalismo,* aqui já retratado, que elevou a proteção de dados sensíveis à esfera constitucional sob o princípio da dignidade humana, cuja proteção, levou o Direito a um novo patamar de discussão.

Assim, a busca de modelos regulatórios dessas tecnologias, tem ocorrido de modo avançado na União Europeia, inclusive, estabelecendo restrições legais ao uso de *softwares* ou *hardwares,* que produzam decisões *exclusivamente automatizadas*[79], como meio de frenar inovações tecnológicas que apresentam grandes riscos. (SILVEIRA, 2022)

Nessa direção, diversos princípios éticos passaram a ser concebidos como pilares do direito na implementação de IA, contudo, havendo ainda a carência dessa realidade no jurídico do Brasil e em muitos países da América Latina, que sustentam suas discussões, inicialmente, a partir das construções regulatórias da União Europeia e dos EUA.

As nações tecnologicamente avançadas, por sua vez, correm para estabelecer expertise e hegemonia no desenvolvimento de tais tecnologias de IA, como vantagem competitiva no plano econômico, e também, no âmbito bélico; portanto, construindo das normativas regulatórias e éticas, que servem de alguma forma, como inspiração e caminho inicial para uma abordagem regulatória em outros países do mundo, a exemplo do Brasil.

5.1.1 Percepção sobre Inteligência Artificial no Brasil e na América Latina

Como revela o Banco Interamericano de Desenvolvimento (BID, 2020; p.34) esta questão ética sobre uso da inteligência artificial, encontra-se em estágio incipiente na América Latina e no Caribe, havendo ainda carência de informações robustas sobre implementação e reflexos, contudo, em pesquisa com parceiros regionais, suas descobertas retrataram que:

> a) 58 % dos parceiros estão considerando pouco, ou muito pouco, o uso de IA para atingir seus objetivos;
>
> b) 62 % acreditam que o tema ética da IA está ausente, ou tem pouca presença, no debate público;
>
> c) 40% possuem a percepção de que o setor privado tem maior influência nas discussões sobre IA, enquanto 29% sustenta que é o acadêmico;

[79] CEPEJ (2018).

d) 56% dos usuários refletem que os problemas éticos ligados a inteligência artificial estão condicionados as questões de privacidade e segurança do usuário; enquanto 37%, acredita estar ligado à confiabilidade e segurança do sistema;

e) a maioria dos envolvidos na pesquisa nunca viram casos implementados de IA para o *bem social*, estes na ordem de 70% dos parceiros que responderam a pesquisa.

Não obstante, as percepções sobre a IA direcionada ao bem estar social realizada pelo BID (2020), diversos organismos estão realizando esforços para regulamentar tais tecnologias para mitigar os riscos já evidenciados, estando na mesa de trabalho da discussão internacional como as mais relevantes sugestões nesse seguimento.

Esses organismos internacionais trabalharam formulando diretrizes e instrumentos para que países membros sejam capazes de promover seus sistemas de inteligência artificial focados nos direitos humanos e no respeito a dignidade de seus povos, assim, como direciona o Banco Interamericano de Desenvolvimento (BID) ao objetivo do bem estar social.

Assim, diretrizes já estão sendo criadas, também, pelo Fórum Econômico Mundial (FEM), a Organização para a Cooperação e Desenvolvimento Econômico (OCDE), a Organização das Nações Unidas para a Educação, a Ciência e a Cultura (UNESCO) e pela União Europeia (UE), além de organizações acadêmicas como o Instituto de Ética em IA da Universidade de Oxford, na Inglaterra, entre outras. (BID, 2020)

Conquanto, mais de 90 (noventa) documentos sobre os princípios éticos da IA já haviam sido publicados em 2019, por governos, empresas e agentes diversos, a exemplo do "*Grupo de Especialistas de Alto Nível em Inteligência Artificial da União Europeia",* mediante incentivo desses organismos, tendo como foco, o incremento da justiça, capacidade interpretativa e de explicabilidade dos sistemas tecnológicos de IA. (BID, 2020, p.33)

Estando à vanguarda das discussões éticas sobre o uso da inteligência artificial, a União Europeia aprovou a *Carta Europeia de Ética*[80] adotada pela *Comissão Europeia para a eficácia da Justiça* (CEPEJ), na 31ª reunião plenária em 03 dezembro de 2018.

Destinada aos setores público e privado responsáveis pela criação e implementação dos serviços de inteligência artificial, traçando diretrizes para impulsionar a gestão das decisões e dados judiciais voltadas a uma espécie de justiça cibernética, com abordagem proativa e repressiva.

[80] Consulte em https://rm.coe.int/carta-etica-traduzida-para-portugues-revista/168093b7e0.

A Carta Europeia objetiva melhorar a eficiência da justiça e identificar formas para implementar a inovação tecnológica de forma responsável, para suas soluções estarem em plena compatibilidade com os direitos individuais consolidados na Convenção Europeia dos Direitos do Homem e visa também fornecer aos tomadores de decisão e servidores da justiça, a melhor compreensão sobre benefícios e riscos do modelo preditivo existente na Inteligência Artificial, tornando-se instrumento norteador direcionado à Europa. (CEPEJ, 2018)

Expôs o RGPD (2016) explicitamente, os princípios éticos a partir da análise minuciosa e aprofundada dos especialistas[81] que têm se constituído como referência, não obstante, outros protocolos estarem paralelamente surgindo e fundamentando iniciativas legislativas e decisões políticas de grande importância social.

É necessário, entretanto, observar nessa regulação inspirada em outros modelos sociais, estabelecer quais os contrapontos axiológicos e valorativos destas normas para a multicultura e diversidade do Brasil, posto que devem fundamentar-se em uma espécie de justiça cibernética ou *ciberética* com potencial de tornar-se referência para legisladores, juristas, estudiosos e a sociedade civil de modo amplo, sem ferir preceitos internos.

É importante que tais princípios mais abrangentes sejam incorporados e adaptados ao contexto multicultural do Brasil, adaptados, contudo, à luz das problemáticas históricas de discriminação racial e social existentes no âmbito pátrio, para incrementar com sucesso uma política inicial de governança ética, atrelada a diversidade cultural e ao desenvolvimento pautado no respeito aos conhecimentos e culturas tradicionais, que de modo preventivo, seja capaz de estabelecer estratégias e processos de tutela da dignidade humana, em sua máxima expressão.

5.1.2 Princípios éticos para regular o uso da Inteligência Artificial

No contexto da Carta Europeia, os riscos do sistema de IA no âmbito judicial é demonstrado pelo caráter *preditivo* que esta tecnologia apresenta, ou seja, sobre a possibilidade de ter que acessar dados dos usuários ao realizar tarefas e decidir preditivamente no lugar dos seres humanos, com capacidade da máquina autônoma.

[81] O Apêndice I da Carta Ética da Europa, apresenta o estudo aprofundado sobre inteligência artificial nos sistemas judiciais com explicações conceituais e técnica, a partir do olhar de diversos avaliadores especializados.

Nessa concepção existe o risco do trabalho judicial se transformar em uma *justiça preditiva,* baseada na técnica de probabilidade a partir de motores de pesquisa no banco de dados, deixando de lado aspectos valorativos importantes.

Assim, a *"disponibilidade de dados é uma condição essencial para o desenvolvimento da IA. [...] Quanto mais dados disponível, mais a IA é capaz de refinar modelos, melhorando sua capacidade preditiva".* (CEPEJ, 2018; p.2)

Com esta preocupação a União Europeia estabeleceu cinco princípios éticos focados no uso da inteligência artificial e dos recursos de algorítimos e preditivos, depurando uma ética inicial desafiadora, tanto para a Europa, quanto para a realidade brasileira, sendo eles:

a) Princípio do respeito aos direitos fundamentais: no trato das decisões judiciais e uso dos dados dos indivíduos com finalidades claras; há aqui a necessidade de respeitar as normativas garantistas existentes sobre direitos fundamentais constantes da Convenção Europeia de Direitos Humanos (CEDH), e da Diretiva (UE) 2016/680, do Parlamento Europeu e do Conselho atinente à proteção das pessoas singulares, no tratamento automatizado de dados pessoais;

b) Princípio da não-discriminação: visando prevenir qualquer discriminação entre pessoas ou grupos de pessoas, pelo processamento de dados baseados na etnia, orientação de gênero ou sexual, fé religiosa ou filosófica, condições de classe ou socioeconômicas, filiação sindical, opiniões ou inclinações políticas, além de condições de saúde, como elementos decisórios de máquina;

c) Princípio da qualidade e segurança: para que processem decisões judiciais e dados, visando operar em ambiente de software ou de hardware protegido, de modo a evitar intervenções ou alterações de dados no uso de tecnologias, além de permitir o rastreamento do processamento dos dados;

d) Princípio da transparência, imparcialidade e equidade: estabelecendo-os como método de tratamento dos dados verificáveis. Busca-se nesta discussão, encontrar o equilíbrio entre a propriedade intelectual e a necessidade de transparência do sistema, posto que para haver imparcialidade e integridade do sistema é necessário abertura dos códigos-fonte, normalmente limitados pelos institutos de segredo industrial;

e) Princípio do controle do usuário: visa garantir ferramentas que permita fazer suas escolhas de maneira informada e autônoma, com linguagem acessível e adequada.

É de bom alvitre reforçar que essa Carta Ética coloca em discussão a transparência e combate a *opacidade* dos sistemas e modos decisórios das máquinas e enaltece a importância do rastreamento das fases da IA, para garantir a integridade do sistema e sua segurança, a partir do monitoramento.

Há, entretanto, forte pressão empresarial inerente o direito de propriedade intelectual utilizadas por grandes empresas de tecnologia que se negam a fornecer códigos-fonte abertos dos seus sistemas para que tal acompanhamento se realize, sob escusa de *sigilo industrial* sobre suas inovações tecnológicas.

Não obstante, essa normativa surgida após o RGPD (2016), regulamento de proteção de dados europeu, teve o papel de fortalecer a proteção de dados sensíveis e empoderar o usuário diante das grandes empresas de tecnologia, gerando maior autonomia no gerenciamento e controle dos dados pessoais, sendo positivo instrumento de prevenção.

Outro ponto fundamental foi o de provocar o papel pedagógico por parte dos implementadores de IA estimulando a promoção de educação em tecnologia da informação aos usuários, visando reduzir questões ligadas a nocividade que se apresenta na engenharia social, ou seja, a que ocorre a partir da dificuldade e desconhecimento do usuário no ambiente digital, fato que lhe ocasiona riscos.

Nessa direção, de modo a ampliar o olhar além do estabelecido pela União Europeia, também foram estruturados requisitos éticos em 2019, pela Organização para a Cooperação e Desenvolvimento Econômico (OCDE, 2019a), sob o lema "*melhores políticas para melhores vidas".* Este importante organismo internacional atuou no sentido da defesa e formalização de conteúdo ético normatizado para ser implementado e respeitado na implementação de IA pelos seus países-membros, sendo iniciativa importante no seguimento.

Essa normativa da OCDE[82] foi acolhida por 42 (quarenta e dois) países, como o Brasil, Chile, Argentina, Colômbia, Costa Rica, Peru e México, estes da América Latina (BID,

[82] O Brasil requereu *acessão* à OCDE e o pedido está em fase de avaliação, contudo, após eleições para Presidência da República e nova governança a partir de Jan./2023, tal perspectiva pode ser alterada. Compõem a OCDE os países: Austrália, Áustria, Bélgica, Canadá, Chile, Colômbia, Coreia, Dinamarca, Finlândia, França, Germânia, Grécia, Irlanda, Islândia, Israel, Itália, Japão, Letônia, Lituânia, Luxemburgo, México, Noruega, Nova Zelândia, Países Baixos, Polônia, Portugal, Reino Unido, República Checa, Eslováquia, Eslovênia, Espanha, Estados Unidos, Suécia, Suíça, Turquia e Hungria.

2020, p.33); reforçando, entretanto, que o Brasil ainda está em estágio de avaliação para *acessão* nos quadros da OCDE, logo, já aderindo aos preceitos de governança e, obrigado-se, por consequência, a corresponder aos princípios de Inteligência Artificial adotados para o bem estar social, como diretriz daquela organização.

Diante da realidade, o Brasil deve instituir as mesmas salvaguardas no cenário da inteligência artificial da OCDE, que possibilitem a intervenção humana sempre que necessário, além de informar aos possíveis prejudicados, os critérios que serviram de base para a *previsão, recomendação ou decisão algorítmica* como meio de tutela de direitos.

Assim, segundo a OCDE (2019), os sistemas de IA devem:

> a) Promover o crescimento com inclusão, pautando-se no desenvolvimento sustentável e no bem-estar social;
>
> b) Ser projetado para respeitar o Estado de Direito, os direitos humanos, os valores democráticos e a diversidade, liberdade, dignidade, autonomia, privacidade e proteção de dados, não-discriminação e igualdade, diversidade, equidade, justiça social e direitos trabalhistas internacionalmente reconhecidos;
>
> c) Funcionar com transparência e explicabilidade (evitando a opacidade), possibilitando informações significativas e apropriadas ao contexto;
>
> d) Possuir sistemas seguros, robustos e protegidos, de modo contínuo, prevenindo riscos potenciais que devem ser continuadamente avaliados, portanto, de modo rastreável para análise do sistema. Assim, a falha prejudicial deve levar a inoperância do sistema;
>
> e) Haver responsabilização pelo funcionamento do sistema a indivíduos e organizações que desenvolvem inteligência artificial; cobrando destes eu estejam de acordo com os princípios estabelecidos; portanto, devem estes serem identificados ou identificáveis para responsabilização.

Nessa direção, Ivar Hartmann (2020, p.8), analisando o relatório da *Berkman Klein Center* da Universidade de Harvard, além dos princípios supramencionados pela OCDE, expõe

que o arcabouço legislativo do Brasil precisa considerar aspectos igualmente importantes, como os princípios a seguir:

> a) da privacidade: segundo o autor em um conceito amplo de consentimento, controle sobre os dados sensíveis, "capacidade de restringir o processamento de dados e direito a correção ou retificação destes, como também, seu apagamento;
>
> b) da equidade e não-discriminação: com objetivo de prevenir os vieses (sesgos) na tarefa algorítmica, em especial, diante dos grupos mais marginalizados, portanto, requerendo bases de dados atualizados, com qualidade e representativas, naturalmente de modo a fomentar o tratamento equitativo e imparcial;
>
> c) do controle humano sobre a tecnologia: de modo a proteger a autonomia de escolha dos seres humanos, definindo quais decisões será delegada ao sistema de inteligência artificial; não obstante, resultando na possibilidade de revisão humana da decisão automatizada.

Não obstante, é importante estar atento também aos princípios éticos considerados consensuais considerados pela comunidade científica altamente especializada, que defende cuidados na realização das pesquisas científicas que tenham risco de afetar dados sensíveis, em especial, que envolvam manipulação genética e novas tecnologias.

Reclamou-se, portanto, a convergência conjunta para outros princípios considerados importantes para a pesquisa científica, traçados na *Conferência de Asilomar*[83], na Califórnia, quando especialistas vislumbraram a necessidade de regular para prevenir, com conteúdo ético, os experimentos da biogenética com envergadura de afetar a proteção de dados sensíveis. (HARTMAN, 2020)

---

[83] Em reunião com 140 cientistas norte-americanos e estrangeiros no Centro de Convenções de Asilomar na Califórnia, realizaram discussão sobre a necessidade de criar conteúdo ético sobre os experimentos envolvendo manipulação genética de DNA recombinante, tal sugestão foi publicada pelos pesquisadores nas revistas *Nature* e *Science*, e posteriormente, estabelecidas diretrizes para a proteção à pesquisa e aos pesquisadores cujo documento foi concluído em 23 de junho de 1976; esta reunião tornou-se um marco para a pesquisa cientifica em biogenética pelo conteúdo ético, ficando conhecida como a *Conferência de Asilomar*. (GOLDIM, 1997)

Nesse sentido como expõe Hartman (2020, p.9), indo além do arcabouço de princípios já delineados, com base nos especialistas da *Conferência de Asilomar*, há a necessidade de fundamentar todas as pesquisas cientificas com risco de afetar a proteção de dados sensíveis, princípios que ampliem a transparência e reduza a discriminação, além de criar interação entre os ambitos políticos e científicos na produção de normas e do desenvolvimento científico, como expõe:

> a) o financiamento de pesquisas sobre IA: visando monitorar e garantir o seu benefício diante de situações complexas da sociedade, atrelando-as ao direito, a ética e aos estudos sociais, além das discussões técnicas da ciência da computação e do interesse lastreado meramente nas benesses da economia;
>
> b) a interdisciplinaridade entre Ciência e Política: para constituir troca de informações entre pesquisadores, ampliando a participação da sociedade civil, através de consultas e audiências públicas, com especialistas em IA;
>
> c) produzir transparência judicial: que permita que os sistemas autônomos de IA forneçam explicabilidade satisfatória e auditável por autoridade humana, legalmente competente;
>
> d) Possuir autonomia sobre os dados pessoais: de modo a evitar a restrição injustificada no exercício cidadão e de liberdade destas acessarem, gerenciarem e controlarem seus dados;
>
> e) Permitir a prosperidade compartilhada: cuja economia criada com o uso da inteligência artificial, seja empregada para a melhoria de vida e redução da miserabilidade, beneficiando a humanidade;
>
> f) Atuar para reduzir os riscos impostos pelos sistemas de IA: evitando danos catastróficos ou existenciais, que devem se sujeitar a excelência do planejamento e mitigação de impactos proporcionais aos respectivos riscos.

Nessa direção, atuam as principais "*diretrizes de ética para a inteligência artificial confiável existente na União Europeia foram desenvolvidas por um grupo independente de 52 Especialistas de Alto Nível em IA*" (BID, 2020, p.33), visando regular a apartir de esforços

desses profissionais oriundos do ambiente acadêmico, da sociedade civil organizada e também da indústria, requisitos fundamentais para construção de arcabouço legislativo robusto sobre inteligência artificial.

Não obstante, é imprescindível que as normativas sejam capazes ser capaz de responsabilizar os atores de modo distinto e bem discriminado no serviço de construção da inteligência artificial; considerando as reais divisões de tarefas, diferenciando criadores, implementadores e usuários do sistema. Há, portanto, uma necessidade entre a ética e a técnica, a considerar, além da perspectiva dos financiadores e seus objetivos, como contraponto político.

Assim, a responsabilidade dos criadores recairia sobre a criação e aplicação dos requisitos adequados e éticos ao processo; a responsabilidade dos implementadores, fomentaria a capacidade deste assegurar que o sistema utilize produtos e serviços que cumpram requisitos éticos. (HARTMAN, 2020)

É importante considerar que a máquina pode realizar a *"própria cognição ética",* uma espécie de *moral exótica* ou moral artificial, assunto que deve ser analisado pela equipe técnica de engenharia com profunda interação dos especialistas do Direito, para determinar o estatus de consideração dessa moral, haja vista, que no comportamento humano, este é exigido. (BOSTROM e YUDKOWSKY, 2011, p.207; 211).

Os usuários finais ou sociedade como um todo, por sua vez, passariam a serem informados sobre requisitos e limitações das tecnologias, bem como, atuariam com maior consciência e autonomia decisória no uso das tecnologias, com capacidade de transigir e exigir que direitos sejam respeitados no processo de uso da inovação tecnológica. (HARTMAN, 2020)

Emerge desta análise, a necessidade de um jusfundamento ético do Direito robusto para o Brasil, que possa submeter tanto as grandes empresas de tecnologias, quanto atores individualmente envolvidos no tocante a responsabilidade sobre as *máquinas inteligentes,* criando um ecossistema fomentador de direitos humanos fundamentais, ao contrário de fragilizá-los pela inovação científica.

5.2. PILAR ANTIDISCRIMINATÓRIO PARA O DIREITO

"O direito pode se rejuvenescer apenas suprimindo o próprio passado"
Rudolf Von Ihering (2019, p.30)

O desenvolvimento e a técnica que as tecnologias digitais alcançaram neste início de século XXI, é surpreendente, e apresenta muitos benefícios que são sentidos nas mais triviais tarefas do cotidiano, porém, na mesma intensidade, apresenta riscos de discriminação de grupos vulnerabilizados, a partir das funções algorítmicas existentes nas técnicas de inteligência artificial.

Sendo tais riscos de IA enormes e diretamente proporcionais ao acelerado desenvolvimento que elas apresentam no cotidiano, se faz imprescindível reforçar a necessidade do direito se constituir sob o *pilar jusfundamental antidiscriminatório*, posto que diversos instrumentos regulatórios existentes, como alguns expostos neste trabalho, não trazem a preocupação com o princípio da não-discriminação (*lato sensu*) ou mesmo de um princípio antirracista[84] (*stricto sensu*) na concepção regulatória dessa tarefa algorítmica.

Conquanto, há uma carência de demarcar propositadamente tal fundamento relevante no desenho da IA mundo a fora, reprodução que não pode ocorrer no Brasil, no qual o princípio antidiscriminatório ou da não-discriminação deve ocorrer de modo obrigatório, estando presente no desenho regulatório e na implementação da inteligência artificial em todas as fases, como marcador proposital e expresso, sob pena de regredir a própria história.

É de bom alvitre observar que, alguns regulamentos de IA nada citam sobre prevenção da discriminação; outros documentos o projetam de modo genérico, a partir do respeito ao Estado de Direito e os valores democráticos, sugerindo apenas, a diversidade entre tantos direitos dispersos, a considerar.

Não obstante, algumas normativas já trazem a determinação de prevenir os vieses discriminatórios na tarefa algorítmica, expressando o princípio da não-discriminação diante de grupos marginalizados como fundamento legal, inclusive, exigindo tratamento equitativo e imparcial entre indivíduos; avanços que precisam ser cooptados pelo desenho de IA que o Brasil venha a implementar.

Tal preocupação se dá pela facilidade em que dados sensíveis são cooptados no ambiente digital e como podem ser utilizados para fins escusos, revelando que muitas tarefas comuns escondem verdadeiras armadilhas digitais com objetivo de coletar informações e utilizá-las para vantagens diversas.

---

[84] Antirracista refere-se a concepção sobre antirracismo: *"diz-se de postura, atitude, movimento, prática, etc. que se opõe ao racismo ou o combate."* V. Academia Brasileira de Letras. Disponível em https://www.academia.org.br/nossa-lingua/nova-palavra/antirracista. Acesso em 07 Dez. 2022.

As tecnologias de vídeo monitoramento para captação biométrica, por exemplo, e uso de sensores de reconhecimento facial[85], *big data,* uso de algorítimos com base em banco de dados com informações sensíveis das pessoas, além dos processos decisórios a partir de máquinas inteligentes, escondem nos bastidores uma infinidade de possibilidades discriminatórias a partir das tarefas que realizam.

Tarefas aparentemente banais no uso dos recursos digitais, como colocar um simples filtro para fotografias ou tirar *selfies* em um *smartphone,* um jogo para captar dados biométricos do corpo das pessoas ou mesmo testes de personalidade nas redes sociais que são estimulados enquanto modismo cultural, escondem como pano de fundo, uma gama de interesses organizacionais que se manifestam para cooptar dados sensíveis dos usuários de diversas formas, de modo inocente.

Por vezes*,* a moderação de conteúdos de redes sociais para obter informações privilegiadas dos usuários, cujas informações retratam sobre a capacidade de crédito desses, ou mesmo, selecionam trabalhadores ou candidatos a consumidores, a partir de características físicas específicas, notadamente informadas nos formulários de uso das plataformas digitais; as máquinas inteligentes formam perfis e inferências sobre as pessoas, com base nas características de cor, moradia, sexo, religião, gostos e condições econômicas.

Outra prática comum é o monitoramento dos locais que os usuários costumam frequentar, a partir do qual lhes são sugeridos um ecossistema de consumo, mas que também, pode servir para possível localização com alto nível de acerto ou mesmo para medir o desempenho no âmbito laboral de determinado funcionário, por tudo, podendo apresentar vieses discriminatórios no trato dos dados do usuário, em várias situações do cotidiano.

Tais ferramentas são efetivamente poderosas para diversos fins, inclusive, para as organizações criminosas, como visto no desenvolvimento dos crimes cibernéticos, pelo qual afetam dados sensíveis para obter vantagem indevida, contudo, direcionar exclusivamente a IA para boas práticas sociais como na medicina, no comércio e na oferta de serviços financeiros personalizados, é o grande desafio do momento.

5.2.1 A inteligência artificial pode promover antidiscriminação algorítmica?

O instrumento nocivo de discriminação algorítmica pode afetar grupos inteiros vulnerabilizando-os, a partir do trato de informações sensíveis dessas populações e a criação de

[85] Formalmente denominadas de Tecnologias de Reconhecimento Facial (TRF).

vieses cognitivos que podem desfavorecer alguns grupos em detrimento de outros, a depender da manipulação política ou ideológica da seletividade que se deseje realizar.[86].

Nesse sentido, Ana Frazão (2021) revela que tecnicamente a discriminação algorítmica se processa por meio estatístico, um processo de *discriminação estatística,* no qual o usuário é julgado pelas características inerentes ao grupo étnico, de classe ou religioso ao qual pertence, sem recurso para que possa haver alguma individualização de suas condutas.

A capacidade de replicar a inteligência pela máquina possui limitações tecnológicas, portanto, nessa atividade não possui condições de fundamentar seus resultados em qualquer ética, há impossibilidade atual da máquina simular um modelo de ética, nos moldes da ética processada pelo complexo cérebro humano.

O cérebro humano apesar das experiências e preconceitos existentes possui capacidade de compreensão para frenar ações e tarefas, a partir do julgamento de contextos sociais relevantes, portanto, sendo mais confiável para gerenciar a vida humana, que a máquina algorítmica no trabalho autônomo.

Note que muitos resultados algorítimos discriminatórios podem ser construídos de modo proposital *a* partir de uma seleção de usuários com determinado perfil específico e objetivo de determinado projeto. Como também, podem surgir a partir de resultados algorítimos aleatórios que a própria máquina produziu (de modo autônomo em um processo decisório sem a intervenção humana), destoando, da programação inicial dos engenheiros.

Os problemas evidenciados na discriminação estatística tendem a acontecer mesmo quando os dados inseridos no banco de dados estão corretos ou mesmo com estatísticas adequadas, assim, os algorítimos tendem a vislumbrá-los como um padrão, porém, na replicação tendem a falhar por algum elemento do processo que não foi possível obter controle. (FRAZÃO, 2021)

A qualidade dos dados constantes dos bancos utilizados pelos sistemas algorítmicos existe uma dificuldade de compô-los com segurança, seja pela velocidade das alterações tecnológicas, seja pelas preferências e hábitos dos usuários que se modificam constantemente,

[86] Durante a guerra da Rússia, o tema *convocação de soldados* pela Agência de Segurança Federal, tem sido objeto de preocupação pelos órgãos internacionais de direitos humanos, em razão das denúncias da Ong *OVD-Info, projeto de mídia independente de direitos humanos da Rússia,* sobre o modo de seleção de pessoas; segundo as denúncias, estão sendo convocados jovens *muito novos, desempregados e pobres*, além de *presidiário*s, na maioria que não são reservistas do exército, demonstrando a seletividade discriminatória no perfil dos convocados. Disponível em https://data.ovdinfo.org/chronicles-anti-war-repressions-eight-months-war#8 e em https://areferencia.com/europa/russia-tem-recrutado-presidiarios-para-reforcar-seu-exercito-afirma-ong/. Acesso em 23 Nov. 2022.

funcionando como um ruído importante que pode comprometer determinados grupos, inclusive pela falta de atualização das fontes de informações (FRAZÃO, 2021)

Não obstante, tornam-se ainda mais preocupantes, os resultados algorítimos quando as informações que alimentaram o sistema não são de qualidade ou se baseiam em condições históricas discriminatórias, gerando previsões ou resultados preditivos viciados.

A discussão se torna perceptível segundo o relatório do observatório de segurança da Universidade Cândido Mendes, no monitoramento de ocorrência de homofobia, racismo, discriminação religiosa, abusos no sistema penitenciário, entre outros; que demonstrou após cinco meses de monitoramento das prisões a partir do reconhecimento facial, que estas continham registros de raça e cor, sendo que "*90,5% das pessoas eram negras e 9,5% eram brancas"* (RAMOS, 2019; p.69), revelando um sistema nocivo de IA que reconhece, prioritariamente, negros como criminosos, suscetíveis de discriminação a partir da tecnologia.

Na mesma direção, expõe Silva (2022), que as buscas no site de pesquisa *Google* reconheceram ferramentas de trabalho nas mãos de pessoas negras como *arma de fogo,* revelando a tendência preditiva dos algorítmos para a construção de um perfil agressivo dos negros, com o efeito de favorecer a criminalização destes, diante das políticas criminais.

Outras aberrações similares foram elencadas por Silva (2022), que passou a traçar uma linha do tempo, evidenciando outras ocorrências:

- foi identificado diferença nos valores que anfitriões brancos pagam em relação a não-brancos, nas plataformas de hospedagem;
- desenvolvedores denunciaram que o reconhecimento do *Googlephotos* marcou pessoas negras como 'gorilas' e o *Facebook* rotulou como 'primatas' vídeos com homens negros;
- o programa *Compas* de predição da criminalidade, foi denunciado por errar e auxiliar réus brancos, além de prejudicar, réus negros;
- o sistema de anúncios do *Facebook* permitiu excluir usuários por raça (latinos, negros e asiáticos), fato que é considerado ilegal nos EUA;
- na análise da expressão facial das plataformas da *Microsoft* e *Facebook* estas associaram vieses negativos às pessoas e atletas negros; bem como, negros tiveram suas faces marcadas como os menos felizes e os mais raivosos;
- *Instagram* gerou registro de falso, em um post legítimo de uma socióloga, que dissertou sobre o conceito de branquitude;
- Algorítmos utilizados na identificação de pessoas relacionou as falas comuns de negros ao discurso de ódio*;* e no *Google perspective,* utilizado como moderador de conteúdo, a linguagem afro-americana vem sendo discriminada;

- o *Canva*, site de criação de anúncios e artes, apresentou somente noivas brancas nas 12 primeiras páginas de resultados, após a busca;
- filtros da base de dados *"Colossal Clean Crawled Corpus"* (corpos rastreados para limpeza colossal), exclui mais documentos relacionados a autores negros, hispânicos e do grupo LGBTQI+;
- usando a técnica de *Deepfake*, recurso de modificação de vídeos, desenvolvedor substituiu a imagem de atriz negra (Chloe Bailey) por uma atriz ruiva no trailer do filme "*A Pequena Sereia".*
- Mulher negra dando aula no recurso de busca do *Google direcionou* usuários para páginas de pornografia*s;* o mesmo ocorreu nas buscas relacionadas às mulheres negras, em geral.

Há de se observar que os algorítimos discriminatórios relacionaram homens negros a uma posição errônea, animalesca e de agressividade, como se estes fossem tendentes ao desequilíbrio emocional e a violência, na comparação a outros públicos.

As mulheres negras tiveram seus conteúdos na internet interrelacionados ao ambiente da sexualização de suas condutas, ademais, foram estas mulheres invisibilizadas como destinatárias dos casamentos formais ou mesmo para estrelar como protagonistas de filmes ou destinatárias da fama cinematográfica.

Esses eventos evidenciados na realidade da IA, tem demonstrado a fragilidade dos empregos do sistema algorítmico diante das discriminações raciais e de gênero, posto que demonstram vieses discriminatórios que precisam ser geridos e eliminados na tarefa.

Ademais, importante compreender que quando os algorítimos atuam de modo autônomo, por vezes, com base de dados impregnada de preconceitos raciais e sociais, ou mesmo a partir de engenharias técnicas mal estruturadas, surge o estímulo à discriminação, a partir de vieses algorítmicos discriminatórios fruto da decisão de máquina.

Do mesmo modo discriminatório, o uso dos algorítimos podem afetar consumidores do ponto de vista econômico e no âmbito do consumo, por meio da geoprecificação (*geopricing)* e geobloqueio (*geoblocking)*, privilegiando técnicas predatórias de captação de clientes e lucro (FRAZÃO, 2018); sendo que a depender dos dados da condição econômica e local de moradia dos indivíduos ou do modo de consumo destes, os sistemas de inteligência artificial geram resultados distintos na precificação de produtos.

Nessa realidade, há uma opacidade (falta de transparência) e a carência na responsabilização *(accountability)* dos sistemas que utilizam algorítimos, tornado-se um instrumento de poder perigoso, que pela falta de informações adequadas restringe os usuários no direito de transigir, questionar ou mesmo impugnar os resultados.

A obrigatoriedade em aceitar qualquer resultado nessa técnica de precificação e geobloqueio, aceitando qualquer resultado possível, podendo ocasionar aumento de pobreza e acentuar a violação do bem estar social, daí a importância da regulação do direito sob o aspecto ético e além, antidiscriminatório, no trato dessa tecnologia. (FRAZÃO, 2021);

Como revela, Bostrom e Yudkowsky, (2011, p.203) se a máquina *"substituir o julgamento humano de funções sociais",* é necessário que ela também seja cobrada quanto a sua ética e modos de construir resultados, para prevenir discriminações na função algorítmica, logo deve promover uma atuação tecnológica que promova elementos antidiscriminatórios.

Hartmann Peixoto (2021), reforça que a inteligência artificial deve estar atrelada a princípios substanciais ligados à justiça, associando o viés técnico ao direito e ao princípio do devido processo legal, com foco na justiça social e dentro da lógica da cooperação.

Os recursos preditivos, que realizam o trabalho de previsão de resultados, por sua vez, não podem ser indiscriminados, e deve considerar os riscos e os impactos da implementação dessas técnicas de IA, além de ter a capacidade de reversibilidade de danos, se estruturando enquanto um sistema de gradação de responsabilidades bem definidas. (HARTMANN PEIXOTO, 2021).

O sistema de inteligência artificial de um país cujo fundamento é o Estado Democrático de Direito, pautado na igualdade social e que possui como corolário do Direito Constitucional a Proteção de Dados Sensíveis como jusfundamento do ordenamento, deve fomentar o aprendizado de máquina para ações e tarefas antidiscrminatórias, retroalimentando seus sistemas internos ao longo do tempo.

Cada indivíduo possui o direito ao exercício da cidadania e das liberdades públicas que deságuam na capacidade de aperfeiçoar suas próprias vidas, *não* podendo sofrer indiscriminadamente os resultados preconceituosos, racistas ou sexistas dos instrumentos tecnológicos de inteligência artificial, por afetar a perspectiva da *democracia digital*[87].

Assim, a IA e a técnica de seus algorítimos, exigem a resistência à manipulação de dados para interesses escusos (BOSTROM e YUDKOWSKY, 2011, p.202); devendo apresentar atributos sérios para prevenir abusos no uso das tecnologias, em especial, diante da superconectividade digital e na análise da inteligência artificial, que não pode tornar-se mais um instrumento de dominação e poder de uns povos pelos outros.

[87] Democracia Digital é termo utilizado por Tarcízio Silva na obra **"***Racismo algorítmico: inteligência artificial e discriminação nas redes digitais"*, para marcar teoricamente que o *Democrático Estado de Direito* também precisa estar presente no âmbito digital. (SILVA, 2022)

Desenha–se neste momento, um estágio importante para o Brasil no tocante aos estudos sobre direito e inteligência artificial, posto que este desenvolvimento tecnológico tem se apresentado como vantagem competitiva em diversos aspectos no mundo, com dois caminhos distintos na produção do conhecimento sobre esta temática.

De que as normativas de IA devem ser pensadas, também, a apartir de populações alijadas e excluídas do processo de formação do conhecimento ocidental ao longo do tempo, não podendo ser exclusivamente das nações europeias, de modo monocultural.

Portanto, a IA para ter uma aplicação antidiscriminatória, precisar levar a discussão regulatória do Brasil às minorias, de modo a construir normativas que considerem a própria cultura brasileira e a diversidade de seu povo.

Como revela Hartmann Peixoto (2021), este é o momento crucial para contribuir para a comunidade internacional, ou tornar-se mero espectador e reprodutor das normativas construídas por agentes internacionais eurocêntricos.

É preciso observar que muitas tecnologias digitais emergentes têm priorizado ideais de lucro de grande escala e as minorias raciais, em todo o mundo, estão ficando alijadas das benesses tecnológicas, sendo submetidas ao monitoramento tóxico com potencial discriminatório que afetam as democracias. (SILVA, 2022); ter a mola mestra das decisões antidiscriminatórias e capacidade técnica para coibir tal potencial, se faz deveras importante.

Torna-se, portanto, construir conhecimento científico sobre IA e em correlação com a ética e o Direito, de modo a construir atributos que permitam o desenvolvimento da tecnologia, mas que tenha o condão de prevenir discriminações ou uso de vieses algorítimos, com atenção especial, a história de escravização e genocídio dos povos negros e índios que o país produziu, e que reflete na desigualdade social e racial, até os dias de hoje.

Antes, contudo, é preciso conhecer como se deu historicamente a formação do pensamento ocidental e da construção do Direito no Brasil e nos países Latino Americanos ou *Amefricanos*[88], para que de modo ambicioso, fomente-se a construção cientifica a partir da regulação multicultural, antirracista e não-discriminatória.

Que considere a cultura dos sujeitos de direitos historicamente excluídos da formação do conhecimento e das decisões coletivas, na construção dos requisitos regulatórios e dos princípios éticos de IA, refletindo a prevenção das desigualdades brasileiras.

---

[88] *Amefricano* é termo criado por Lélia Gonzalez (1982) que se refere à contribuição cultural das mulheres e homens negros oriundos da África e traficados para as Américas, na diáspora; tal termo, vai além de uma mera designação geográfica e atua para combater a visão sexista, racista e elitista que nega a imensa contribuição social e cultural da população negra, considerando exclusivamente, à contribuição da comunidade branca.

5.2.2 Técnicas antidiscriminatórias para regular os algorítmos de IA

O importante pilar antidiscriminatório do direito visa promover a proteção e tutela dos indivíduos em sua diversidade, a partir da proteção dos dados sensíveis e da privacidade, além do livre consentimento, atuando de modo previsível para prevenir o racismo, o sexismo e o genocídio dos povos historicamente excluídos, inclusive, prevenindo a formação de novas formas de discriminação.

Assim, importantes são os critérios necessários, mas não exaustivos, ao sistema de IA no emprego de algorítimos matemáticos destinados a realizar tal substituição das funções humanas, retratadas por Bostrom e Yudkowsky (2011, p.203), cujas técnicas de controle podem contribuir para evoluir o sistema ao ponto de prevenir discriminações, sendo elas:

> a) Responsabilidade: estabelecendo as divisões de trabalho sobre criação e implementação de IA, de acordo com objetivos, estabelecendo meios de responsabilização proporcional;

Em todas as fases deve haver o rastreamento das funções algorítmicas nas três partes principais que formam a IA, na fase do *data set* que se refere a alimentação dos dados, onde o sistema é alimentado, ou seja, a porta de entrada para futuros problemas de vieses; portanto, tendo importância em estabelecer a qualidade e historicidade dos dados que farão parte do banco de informações.

A fase dos arranjos algorítimos onde se concentram as maiores criticas sobre possíveis vieses discriminatórios e na *fase dos resultados* onde os erros devem possuir mecanismos de segurança, além do acompanhamento contínuo e reavaliação de resultados, para promover técnicas mais apuradas. (HARTMANN PEIXOTO, 2021)

> b) Transparência: evitando a *opacidade*[89] sobre os processos e como os algorítimos tomam decisões ou mesmo conhecer adequadamente como se processam as fases de construção da decisão algorítmica, para evitar erros especialmente na atividade autônoma, na qual o ser humano não interfere;

[89] O termo *opacidade* é utilizado na discussão para designar a falta de transparência total no funcionamento de algorítimos da IA, designando que ainda há informações a serem vislumbradas, mas que não está sendo efetivamente colocado para o público em geral, seja por dificuldades técnicas ou por protecionismo empresarial.

O sistema de IA necessita ser construído sob engenharias de computação que se relacione com a área jurídica como meio de equilibrar as questões regulatórias que apresenta, inclusive, como é construída a IA, para compreender a necessidade da arquitetura interna ser monitorada. (HARTMANN PEIXOTO, 2021)

> c) Auditabilidade: capacidade de rastreamento e de conferir todas as fases do sistema, verificando possíveis erros e falhas ou ainda, identificando algorítimos nocivos ou que demonstrem distorção quanto aos vieses considerados adequados;

Nesta técnica, é possível inclusive, desautorizar a utilização de determinado algorítmo ou técnica de inteligência artificial; tal controle, entretanto, tende a contrariar a autonomia de máquina pois depende da participação humana na supervisão, regulação que por vezes, fulmina o interesse desmedido e ambicioso de grandes organizações empresariais.

> d) Incorruptibilidade**:** considerando que a máquina pode atuar de modo independente do estabelecido pelos programadores, mesmo tendo sido realizado tudo adequado tecnicamente, há o risco de haver um resultado diferente a partir das operações internas dos algorítimos;

É importante observar e monitorar o sistema todo o tempo em todas as fases, evitando ou identificando imediatamente qualquer corrupção do sistema, quando este fugir do nível de segurança adequado, logo, interferindo no programa quando fugir a previsibilidade.

> e) Previsibilidade*:* refere-se a necessidade de conceber comportamento seguro do sistema de IA, operando em contextos diversos e em todas as suas fases, desde a programação, implementação e execução, inclusive, quando atuar de modo exclusivamente autônoma em relação a intervenção humana;

Exige-se aqui que haja garantias de segurança na engenharia dos algorítimos que considerem a possibilidade da máquina desenvolver atuação previsível, que não destoe dos objetivos para os quais foram programados.

Ocorre que, tecnicamente, os algorítimos impõem incertezas nos seus resultados, havendo grande imprevisibilidade tanto de conceber decisões para uma IA amigável ou mesmo

hostil, portanto, constitui-se um *risco existencial*, a utilização de algorítimos autônomos, posto a imprevisibilidade, da intervenção e monitoramento humano. (BOSTROM e YUDKOWSKY, 2011, p.218).

> f) Tendência em não fazer vítimas inocentes: a utilização de recursos tecnológicos devem atuar dentro dos limites da inviolabilidade das pessoas civis, assim sendo, os recursos de geolocalização, algorítimos, reconhecimento facial, *big data* e inovações que permitem o lançamento de drones bélicos e mísseis à longa distância, não devem ser utilizados como vantagem competitiva de dominação contra inocentes, nem mesmo em guerras e conflitos formalmente declarados.

Nessa esfera, acredita-se que a proteção de inocentes deve tornar-se objetivo expresso e primordial de qualquer tecnologia por mais avançada que seja, tendo qualquer tipo maior ou menor de benefício social; quando os riscos da IA alcançam esse estágio de violação, as discussões geopolíticas ou conflituosas entre Estados, precisam estar em segundo plano e a regulação do Direito precisa ter a força necessária para instar, como *ultima ratio*.

Há que ressaltar que não existe no sistema de IA ou mesmo na aplicação algorítmica atual, qualquer ética ou *moral artificial* que venha a coibir tais tarefas de serem realizadas; a possibilidade de IA com habilidades maiores que as humanas, com uma *superinteligência,* apta a gerar um comportamento *superético* diante de tais discussões*,* ainda se constitui um desafio visionário que não é possível neste estágio tecnológico. (BOSTROM e YUDKOWSKY, 2011, p.218).

Na mesma direção, de modo a complementar sobre os requisitos de Direito sob o pilar antidiscriminatório para regular a IA, nessa discussão é importante também lançar olhar sobre como estão sendo construídos os regramentos sobre essas tecnologias no mundo, de modo que possa prevenir uma construção sob o viés monocultural exclusivamente eurocêntrico sobre os algorítimos e outras técnicas.

É importante conhecer para melhor discernimento, que o pensamento ocidental foi afetado historicamente por genocídios de diversos povos, que fundaram uma estrutura epistemológica colonialista, racista e sexista sobre esses grupos discriminatoriamente considerados inferiores. (GROSFOGUEL, 2016, p.43)

Tal realidade levaram as universidades e as pesquisas científicas a se constituírem sob o pensamento majoritariamente de países europeus, privilegiados na formação do

conhecimento, desprezando as culturas desses outros povos que muito tinham a ofertar culturalmente. (GROSFOGUEL, 2016).

O conhecimento e a cultura oriunda dos povos negros, mulheres, muçulmanos e judeus foram mitigados epistemologicamente, na produção da ciência, mitigando a contribuição destes na formação do pensamento ocidental de modo livre e amplo a partir de modelos escravagistas e de exploração.

> O racismo/sexismo epistêmico da estrutura das universidades ocidentalizadas e do mundo moderno ao genocídio/epistemicídio contra muçulmanos e judeus na conquista de Al-Andalus, contra povos nativos na conquista das Américas, contra povos africanos na conquista da África e a escravização dos mesmos nas Américas e, finalmente, contra as mulheres europeias queimadas vivas acusadas de bruxaria. (GROSFOGUEL, 2016, p.25)

Assim, os principais povos atingidos foram os negros africanos, os índios americanos, os muçulmanos e judeus, além das mulheres subalternizadas pela dinâmica machista e sexista, todos com algo em comum, relativo à diversidade de suas culturas e modos de vida, em relação aos seus colonizadores.

No Brasil, atingindo de sobremodo os índios e a população negra, o discurso era de que ambos não tinham capacidades cognoscentes, quanto aos negros especificamente, este era provido de "*falta de inteligência*" e desprovido de alma. (GROSFOGUEL, 2016).

O modelo teórico colonizador branco naturalizava a inferiorização e desumanidade dessas pessoas e contribuía para reforçar o papel de dominação do europeu sobre os negros considerados *rés,* e com suposta, natureza animalesca*,* pelo qual deveriam ser dominados face sua tendência transgressora, enquanto os índios precisavam a todo custo serem civilizados, não obstante, sua escravização.

Estes argumentos utilizados entre os séculos XVI e XX, nas principais teorias científicas do mundo moderno, relegando e inferiorizando a contribuição destes povos na formação do conhecimento ocidental formal, ao passo em que resultou em um privilégio epistemológico branco. (GROSFOGUEL, 2016)

Como exemplo, temos a escravização dos negros africanos transportados sem consentimento próprio para as Américas, a diáspora, que culminou no mais lucrativo e cruel modelo econômico, resultando no genocídio, tortura e sequestro de milhões de seres humanos, estágio mais cruel da história da humanidade.

Para Grosfoguel (2016; p.40), o genocídio desses povos subalternizados, não refletiu apenas a morte dessas pessoas, mas também, a morte de parte da cultura dos

sobreviventes, posto que eram "*proibidos de pensar, rezar ou de praticar suas cosmologias, conhecimentos e visão de mundo",* de produzir e reproduzir seu pensamento multicultural e tradicional livremente, ocasionando além do genocídio, um "*epistemicídio cultural"*[90].

Tais estruturas de dominação permitiram o epistemicídio e prejuízos na construção da ciência moderna sob um pensamento multicultural, pautado na diversidade de experiências, concepções e modos de vida, tendo, contudo, privilegiado o pensamento teórico monocultural europeu, autoritário na produção da ciência, cujo legado foi a desumanização das minorias e exclusão formal do rico conhecimento desses povos que muito tinham a contribuir.

Portanto, na discussão sobre as inovações tecnológicas que se apresentam é necessário considerar nas concepções científicas atuais, a construção de regramentos para a inteligência artificial e algorítimos, que considerem o conhecimento produzido pelas minorias excluídas historicamente; no caso específico do Brasil, que contemple a discussão aprofundada sobre o racismo e sexismo.

Assim, estabelecendo como mais um critério, obrigatório a nosso ver, deve a construção de regramentos sobre IA considerar a diversidade de olhares, a partir de uma discussão multicultural e multirracial, sob pena de sucumbir aos erros do passado e estabelecer vieses exclusivamente eurocêntricos de IA, que pode constituir-se instrumento perigoso e hegemônico de poder.

5.3 PILAR HUMANITÁRIO PARA O DIREITO

> *"A luta pelo direito é um dever do sujeito do direito para consigo mesmo."* Rudolf Von Ihering (2019, p.41)

Iniciamos esse *pilar jusfundamental humanitário* enaltecendo que o ser humano deve ter compromisso com a sua autopreservação e com a lei suprema da sua própria existência, corroborando com o pensamento filosófico de Ihering (2019).

É imprescindível que cada ser social, tenha instrumentos legais e morais para tutelar o projeto humanitário contido na sociedade, que visa a proteção da própria humanidade de cada

[90] Espistemicídio é termo criado pelo sociólogo Boaventura de Souza Santos para designar a *destruição, mitigação ou morte* dos saberes tradicionais, historicamente excluídos da ciência formal, a partir dos vieses coloniais de dominação; favorecendo o conhecimento cientifico restrito a um único modelo epistemológico monocultural eurocêntrico, desprezando a riqueza da diversidade cultural de diversos povos, que contribuíram de fato, para a construção do conhecimento ocidental multicultural. (SOUZA SANTOS, 2009, p.183)

indivíduo, a partir dos valores éticos e direitos fundamentais, que devem estar direcionados ao exercício da cidadania com foco na proteção da espécie humana.

O direito nessa concepção se apresenta como condição existencial e moral dos indivíduos, para que a sua humanidade não seja violada, ou mesmo, estes não venham a tombar ao nível animalesco, pela crueldade dos artifícios de dominação e de poder social.

O direito é relevante justamente pela autoproteção inalienável que promove, como revela Ihering (2019, p.41),*"a afirmação do direito, é portanto, um dever de autopreservação moral [...], do ponto de vista jurídico, tão impossível quanto renunciar ao direito na sua totalidade";* logo, a renúncia da existência física ou moral, representam suicídio moral e renúncia de autopreservação, atuando contra o próprio ser humano.

Assim, as inovações tecnológicas não podem, por mais avançada que sejam, colocar em risco o aspecto existencial do ser humano sob o pretexto de avanço econômico, camuflado em competitividade centrada no dinheiro, desprezando aspectos humanitários, instaurando métodos contraproducentes e predatórios, que expropriam direitos.

O Direito precisa estar apto a ser instrumentalizado diante das violências que surgem contra as pessoas civis no âmbito digital e real a partir das tecnologias, para que não se tornem equipamentos de genocídio e desumanidade, a exemplo do uso de mísseis nucleares e drones contra pessoas civis, como vem ocorrendo na guerra da Rússia e Ucrânia.

Note que no que concerne ao genocídio no plano internacional, o artigo 1º, da Lei nº 2.889 /1956, retrata que este crime se consuma quando:

> quem, com a intenção de destruir, no todo ou em parte, grupo nacional, étnico, racial ou religioso, como tal:
>
> a) matar membros do grupo;
> b) causar lesão grave à integridade física ou mental de membros do grupo;
> c) submeter intencionalmente o grupo a condições de existência capazes de ocasionar- -lhe a destruição física total ou parcial;
> d) adotar medidas destinadas a impedir os nascimentos no seio do grupo;
> e) efetuar a transferência forçada de crianças do grupo para outro grupo. (SENADO FEDERAL, 2013)

Deste modo, considerando que os riscos apresentados nesse trabalho quanto as tecnologias de inteligência artificial, possuem o potencial, nessa dimensão, de mitigar a humanidade das pessoas a partir de vários contextos, uma discussão aprofundada e regulação *antigenocida* é efetivamente necessária.

5.3.1 Inteligência Artificial e a Proteção da Inviolabilidade Civil

No tocante a discussão sobre a violência contra pessoas civis em países em guerra, por força do uso das tecnologias com drones e mísseis comuns já estarem sendo usados para esta finalidade, convém, de modo a contribuir com conhecimento, acrescentar um olhar jurídico também, sobre este instituto.

Nesta direção, a inviolabilidade civil é uma premissa ligada a dignidade do indivíduo e possui um valor fundamental que carrega dentro de si um núcleo valorativo de humanidade, atuando na esfera da dignidade pessoal. (BURKE e SLAUGHTER 2002; p.16).

No regime global, a inviolabilidade civil é protegida desde a Convenção de Haia em 1907, estando na lei de guerra e no direito internacional, cuja Liga das Nações acrescentou instituto em 1938, expressando que "*bombardeio intencional de civil* é instrumento *ilegal"*; ademais, a temática encontra-se nas Convenções de Genebra, sendo que a 4ª Convenção de 1949, trata especificamente da proteção de civis em conflitos armados, limitando e proibindo "*matar e ferir traiçoeiramente*", não-combatentes. (BURKE e SLAUGHTER, 2002; p.6)

Em decisões modernas do Tribunal Penal Internacional (TPI), em 2000, a câmara de julgamento construiu a jurisprudência de que a inviolabilidade civil é *"o alicerce do direito humanitário moderno*" e que os Estados e pessoas devem ser responsabilizados por ataques a pessoas civis, como *crimes contra a humanidade* ou *crimes de guerra*, reconhecendo que pessoas inocentes não podem ser punidas por ações dos seus governantes. (BURKE e SLAUGHTER, 2002; p.8)

Na discussão sobre uso das tecnologias, como ponto fundamental desta análise, os Estados não podem abusar do seu privilégio e desenvolvimento em armas superpotentes e agir fora do princípio da proporcionalidade, ainda que suas tecnologias sejam construídas com o intuito de matar e que o regime de armas seja para submeter o inimigo, não obstante, deve desconsiderar a inviolabilidade das pessoas civis sob qualquer pretexto, o que não vem ocorrendo na experiência atual.

As ações de um governo que contra-ataca a partir do estado de direito e poder de polícia, deve ser evidentemente distinta de um mero terrorista, posto que no solo de guerra o reconhecimento da inviolabilidade civil é imprescindível, portanto, limitar governos energéticos se faz necessário. (BURKE e SLAUGHTER, 2002; p.20)

Assim, na ofensa deliberada e fora dos requisitos adequados de guerra, o direito deve ser instrumento hábil a ser utilizado diante de possíveis abusos desenfreados que surgem, extrapolando a normativa e dando suporte aos órgãos de proteção para atuarem no plano fático.

Portanto, na análise dessa transição tecnológica do século XXI cuja a IA se desenvolve, enquanto parte dessas inovações se demonstraram positivas ao bem estar social, outras vem aprofundando de modo excludente, a produção do conhecimento tecnológico, direcionando-os como instrumento de dominação hegemônica, tendo por pano de fundo, planos geopolíticos.

Nessa direção, as normativas de proteção da humanidade, construídas em sua maioria após a segunda guerra mundial, vem sofrendo críticas por não serem, mais competentes na totalidade a regular esta atual dinâmica da sociedade, nem diante da *smartificação da vida*, da digitalização global, nem no campo da ética de guerra, havendo brechas que demandam atualização legislativa e comprometimento com o projeto humanitário global e o papel do direito nesse contexto.

Para Juana María Gil Ruiz (2022) ao tecer sobre *o paradigma da ciência jurídica na sociedade digital global,* há uma movimentação do poder a partir de influencia de interesses políticos, ditando o modelo de direito em função do mercado digital, entretanto, é necessário refletir, que tipo de jurista precisa ser formado para empreender o direito de modo adequado, em face da exigência global de regulação dessas inovações pelo direito.

Nesse sentido, é necessário que a sociedade assuma o compromisso dos direitos humanos e dos direitos fundamentais para no futuro os relevantes objetivos do direito, em seus reais valores, não seja perdido. O direito nessa direção é instrumento que serve ao interesse político público com objetivo de justiça e enquanto técnica social, de modo a buscar o estado democrático de direito como premissa e a cultura da paz. (RUIZ, 2022)

O papel do direito na sociedade digital da atualidade implica em regular as nações, em especial, superpotências, para que não atuem livremente no contexto político-econômico, submetendo indiscriminadamente a população, diante da força do poderio que possui, daí, a importância de juristas capazes de discernimento além de normas atualizadas ou mesmo que possa se antecipar as tais dinâmicas.

O direito precisa atuar tanto na existência do encantamento dessas nações repletas de estratégias digitais, de modo a intervir para que haja segurança jurídica, quanto nos desencantamentos, intervindo com contundência, quando os instrumentos dessas potências forem ineficazes para servir a justiça, nesse sentido, o compromisso número um com a erradicação da pobreza deve ser pautado de modo global, conforme exposto na agenda da ONU 2030. (RUIZ, 2022)

No tocante a esse compromisso, a agenda 2030 das Nações Unidas, composta por 17 objetivos de desenvolvimento sustentáveis*,* apresenta-se como um apelo à comunidade

global para preservação da vida, erradicação da pobreza, proteção do meio ambiente e redução das desigualdades sociais, com vistas a garantir que todas as pessoas possam desfrutar da paz e prosperidade. (ONU, 2022)

No âmbito jurídico, o objetivo "*16 – Paz, Justiça e Instituições eficazes"* (ONU, 2022), requer que as decisões judiciais possam promover a paz e a justiça como meta principal, contudo, se a resolução dos problemas advindos da digitalização global tornar-se impossível de resolução, pelo caráter transnacional, deve-se considerar a cooperação internacional para atingir determinado objetivo.

Como pôde ser visto tamanha é a dinâmica das tecnologias de IA em relação ao ordenamento jurídico pátrio e internacional, que salta aos olhos a necessidade de adaptabilidade normativa ou criação de novos regramentos humanitários *globais*, capazes de dar conta dessa nova dinâmica no plano fático.

A aparente sobressalência histórica dos direitos humanos tem escondido uma degradação dos precedentes da dignidade da pessoa humana, em especial, com o advento das constantes agressões ocorridas em função das tecnologias de IA, fato que tem reduzido indivíduos, grupos e povos à condição de sujeitos-objeto, restando mero discurso de direitos humanos, face a submissão à máquina.

O exemplo da obsolência das normativas atuais, é a Declaração Universal de Direitos Humanos (DUDH)[91], considerada fundamento-base de respeito aos direitos sociais, culturais, econômicos e políticos de todos os povos, atuando na busca da paz, da segurança e do desenvolvimento sustentável da humanidade, mas que está sob ameaça nos seus 74 anos de existência como instrumento de direitos humanos com caráter global, e sob os princípios da paz, liberdade e cidadania.

Não obstante, a DUDH *"atuar em conjunto com o Pacto Internacional dos Direitos Civis e Políticos [...] e com o Pacto Internacional dos Direitos Econômicos, Sociais e Culturais [...] , que formam a chamada Carta Internacional dos Direitos Humanos",* abrindo alas para diversas outras normativas seguintes, que foram expandidas no âmbito dos direitos humanos internacionais. (ONU, 2022)

Considerando que é necessário coibir as três grandes ameaças as democracias que existem na atualidade, frente à digitalização da vida: discriminação, desinformação e não-liberdade, os desafios do ramo do direito tornam-se ainda maiores, segundo Belloso (2022).

[91] A Declaração foi proclamada pela Assembleia Geral da ONU em Paris, em 10 de dezembro de 1948, por meio da Resolução 217 A (III), como uma norma programática a ser alcançada por todos os povos e nações, estabelecendo pela primeira vez, a proteção universal dos direitos humanos. (ONU, 2022)

A aprovação da nova Declaração Universal de Direitos Humanos *"Emergentes"* no fórum de Monterrey no México, em 2007, focada nas lutas do início do século XXI, desenvolveu a ideia de humanidade enquanto uma comunidade política de "*gênero humano*", que não existia antes.

Seja pela intensificação do processo de globalização, pelo debate Estado-nação ou pelo fortalecimento do mercado internacional, esta norma visou atualizar a DUDH de 1948, dando-lhe novos contornos quanto a cidadania participativa e empoderamento da sociedade civil diante dos problemas sociais e judiciais. (BELLOSO, 2022)

Não previu, entretanto, essa Declaração Universal dos Direitos Emergentes de 2007, a discussão sobre as novas tecnologias ligadas aos algorítimos e *big data* de inteligência artificial, nem mesmo biogenética, portanto, deixou de ter impacto quanto ao emprego dessas atuais tecnologias no plano global, mesmo diante dos riscos ao direito humanitário.

Esta velocidade das mudanças tecnológicas é um dos aspectos importante desta análise, quando observa-se que apenas quinze anos depois dessa discussão sobre direitos emergentes, esta normativa não é mais suficiente para regular aspectos da Inteligência artificial, das violações humanitárias pelo ambiente cibernético e avanços das máquinas autônomas que realizam tarefas humanas, assim, aquele texto normativo, precisa ser novamente racionalizado sob novo viés das tecnologias da atual ambiência.

Deste modo, diante desta velocidade, deve-se mensurar muito além das benesses da inteligência artificial, como também, os efeitos negativos que se amplificam com a superconectividade pandêmica, smartificação da sociedade, engenharia social, controle estatal e privado dos recursos de monitoramento, além da obsolência da regulação pelo direito.

Racionalizar de modo proporcional sobre os efeitos negativos da inteligência artificial diante da vulnerabilização dos dados sensíveis como objeto de valor comercial, das discussões sobre modificações biogenéticas, nanotecnologia, neurotecnologia, dronificação das guerras, robótica, ciborgues[92], tecnologia 4.0, telefonia 5G, geolocalização, entre outras facetas das máquinas inteligentes, torna-se, portanto, imprescindível nesta dinâmica.

5.3.2 Inteligência Artificial e a Proteção da Cognição Humana

[92] Ciborgue ou *cyborgue* é um neologismo que se refere a um organismo que contém conjuntamente partes orgânicas (de um ser humano) e partes robóticas ou cibernéticas (tecnológicas), visando melhorar as capacidades físicas ou cognitivas do ente.

Tamanha é a preocupação e a realidade de ameaça por parte da inteligência artificial em afetar a capacidade cognitiva do ser humano, que o Conselho da OCDE em 11 de Dezembro de 2019, adotou *Recomendação sobre Inovação responsável em Neurotecnologia,* tornando-se primeiro padrão nesse quesito e tendo o objetivo de orientar governos e antecipar desafios do ponto de vista legal, ético e social ocasionados pelas novas neurotecnologias, de modo a maximizar benefícios e minimizar riscos.

Do mesmo modo, para a OCDE (2019b) é necessário um padrão internacional para a inovação responsável em *neurotecnologia*, para tanto, define nove princípios imprescindíveis nessa discussão, que se concentram na priorização na avaliação da segurança das técnicas que enamoram a neurociência com a inteligência artificial, em especial, para a promoção da inclusão sobre os benefícios, com participação social relevante.

Nessa direção recomenda a habilitação para capacitar órgãos consultivos e de supervisão (com foco na previsão, supervisão e aconselhamento); proteção de dados cerebrais pessoais e outras informações correlatas; promover culturas de administração e confiança nos setores públicos, e também, privados; antecipar e monitor o uso não intencional ou indevido potencial da neurotecnologia, de modo a coibir projetos nocivos à sociedade. (OCDE, 2019b)

Acrescenta que a neurotecnologia oferece de fato um potencial significativo para a promoção da saúde, bem-estar, produtividade e crescimento econômico, podendo auxiliar no tratamento de distúrbios mentais e doenças neurológicas, em ambientes clínicos e não clínicos, contudo, somente deve ser utilizada em situações que demandem clara necessidade médica, posto que a *"convergência entre neurociência, engenharia, digitalização e inteligência artificial (IA) está se tornando um dos principais impulsionadores da inovação",* diante das técnicas tradicionais de tratamento de doenças humanas. (OCDE, 2019b)

Como ponto de destaque, reforça que a neurotecnologia tem trazido a discussão sobre diversas questões éticas, legais e sociais *sui generis,* que tais modelos de negócios terão que superar quanto aos riscos relativos à proteção de dados ainda mais sensíveis, como os *dados cerebrais* diante da busca de aprimoramento humano. (OCDE, 2019b)

Há medo da neurotecnologia vulnerabilizar padrões cognitivos das pessoas para manipulação econômica, comercial, política, marketing, discriminatórias ou que produzam mais desigualdades sociais e mitigação no uso e acesso aos direitos fundamentais relevantes, potencialmente violando a dignidade humana.

Na mesma direção, o G-20[93] visando gerar credibilidade a inovação com foto no ser humano, apresentou a Declaração Ministerial sobre Comércio e Digital e Economia, destacando que a sociedade do futuro precisa estar centrada no ser humano; na liberdade do fluxo de informações, com confiança; no processo de acesso igualitário a inteligência artificial com foto no ser humano; nas posições políticas flexíveis e rápidas quanto à economia digital; na segurança e estabelecimento de metas sustentáveis voltadas à inclusão social. (HARTMANN PEIXOTO, 2020; p.37)

Ponto de análise, que eleva o neurodireito a fazer parte de discussão relevante na construção do arcabouço normativo sobre os direitos humanos emergentes no Brasil, como reforça Belloso (2022), é que pode contribuir para este não estar isolado quanto ao controle das tecnologias para fins democráticos, passando a ter apoio internacional.

Considerando que o Brasil não faz parte do rol das nações subordinadas a OCDE, estando em tramitação e sem garantias que essa adesão irá acontecer diante de modificações da política nacional, as carências legislativas sobre IA, precisam ser supridas no plano pátrio, sendo imprescindível considerar a discussão sobre os novos direitos humanos emergentes e estendidos, que permitam um sistema robusto e confiável de neurotecnologia.

Ademais, cabe ao Brasil além de construir sua legislação pátria, fomentar no plano internacional a proteção cognitiva e cerebral da humanidade, diante do potencial de vulnerabilização que tais sistemas podem refletir na cognição dos seres humanos.

Levando a uma democratização do acesso ao conhecimento de IA pela sociedade civil, para compreender os meandros destas tecnologias, enquanto, o arcabouço normativo se constrói. Não obstante, diante do déficit que existe na participação de fiscalização e auditoria pelos os órgãos formais do Brasil, também se faz necessário ampliar essa participação.

De modo específico, as novas discussões sobre direitos ligados a *neurociência ou neurotecnologias* devem permear o diálogo entre as comunidades cientificas, políticas e médicas, para proteção da cognição humana diante das pesquisas que fomentam a autonomia de máquina para realizar funções cerebrais, sob pretexto de melhoramento cognitivo da humanidade ou para a ciência do cérebro. (GOERING; YUSTE, et. al., 2017a; 2021)

Estabelecer *neurodireitos,* portanto, apresentam-se como fundamentais diante dos possíveis efeitos que a inteligência artificial pode ocasionar sobre a capacidade cerebral da humanidade, e como revelam Yuste; Goering; [et. al.] (2017b; p.161/162), há quatro

[93] G20 é o Grupo de países industrializados e emergentes que mantém um fórum de discussão construtivo sobre estabilidade econômica global. O documento apresentado foi o "*Ministerial Statement on Trade and Digital Economy"*. Disponível em http://www.g20.org. Acesso em 05 nov. 2022.

condicionantes éticas necessárias que precisam ser consideradas quando o tema engloba inteligência artificial e neurotecnologia, cujas ações, precisam ser imediatas:

> a) Privacidade e consentimento: há "*um nível extraordinário de informações pessoais já pode ser obtido a partir de trilhas de dados das pessoas",* que desde 2015 permitem o estudo refinado do comportamento de alguns indivíduos e favorecem algorítmos direcionados a publicidade, calculo de prêmios de seguro, padrões de atividade de neurônios e estado de atenção, por exemplo. É necessário declaração de consentimento e proteção das pessoas a partir da educação "s*obre os possíveis efeitos cognitivos e emocionais das neurotecnologias".* (YUSTE; GOERING; et. al; 2017b; p.161)
>
> b) Senso de identidade: pessoas estimuladas por eletrodos implantados no cérebro tiveram alterada a sua identidade, portanto, o emprego de neurotecnologia deve informar essa capacidade de perturbar o senso de identidade e modificação moral ou legal do senso de responsabilidade pessoal. Nesse sentido, os governos devem proteger as pessoas quanto a integridade corporal e mental e as agências de implementação, devem realizar boas escolhas e ações protegendo os direitos humanos.
>
> c) Argumentação: é necessário evitar que as diferenças sobre a capacidade cerebral torne-se elemento de preconceito, visto que as neurotecnologias podem aprimorar experiências cognitivas, expandindo "*capacidades sensoriais ou mentais*", portanto, interferindo nas normas sociais e nas questões de igualdade, comportando nova forma de discriminação. É importante conceber que a rivalidade e a individualidade são elementos mais fortes em algumas culturas que em outras e as decisões regulatórias precisam estar condizentes com o respectivo contexto cultural, portanto, a análise da proibição ou permissão das neurotecnologias precisam ser objeto de debate social aprofundado. (YUSTE; GOERING; et. al; 2017b; p.161)
>
> d) BIAS: Refere-se a tecnologia capaz de criar vieses discriminatórios por meio da função autônoma da máquina, ocorre *"quando as decisões científicas ou tecnológicas são baseadas em um conjunto restrito de conceitos e normas sistêmicas, estruturais ou sociais, a tecnologia resultante pode privilegiar determinados grupos e prejudicar outros."* As medidas para combater os vieses algorítmicos devem ser o fundamento do aprendizado da máquina, portanto, é necessário que *os "prováveis grupos de usuários (especialmente aqueles que já são marginalizados) participem do projeto de algorítmo",* visando garantir a abordagem preventiva dos preconceitos, desde o início da implementação da tecnologia. (YUSTE; GOERING; [et. al]; 2017b; p.162)

Para garantia desses neurodireitos, acredita-se ser deveras importante a participação da sociedade civil na fiscalização da inteligência artificial, mas também de uma regulação robusta que possa ser instrumentalizada pelas instituições de proteção social.

A Defensoria Pública, Ordem dos Advogados do Brasil, Polícia Federal e Ministério Público, entre outras, podem se valer do pilar jusfundamental humanitário do direito, para cobrar práticas de desenvolvimento da nação, atreladas aos fundamentos de proteção da humanidade, como *prima ratio* filosófica do ordenamento jurídico.

CONSIDERAÇÕES FINAIS

O Brasil precisa construir uma política de não-discriminação algorítmica e de inteligência artificial centrada no bem-estar do ser humano a partir dos limites impostos pela lei; os institutos da competência, da necessidade, proporcionalidade e adequação, na tarefa de proteção da sociedade, precisa permear o processo de regulação das tecnologias de IA a partir

dos pilares jusfundamentais éticos, humanitários e antidiscriminatórios do direito, contrapondo-se à filosofia de lucro a qualquer custo.

Para que a Inteligência Artificial se torne positiva à sociedade, faz-se imprescindível considerar as seguintes concepções:

a. Que no Brasil, de modo expresso, o ordenamento jurídico venha a contrapor-se a qualquer tipo de terror, projeto de poder político, biopoder ou manipulação de massa contra a população, a partir da IA, com atenção especial aos grupos historicamente vulnerabilizados como negros, índios, idosos e mulheres.

b. Incorporar normativas éticas e técnicas transparentes, com sanções que possibilitem a responsabilizando pela violação da privacidade e dos dados sensíveis, inclusive biométricos, neurais e emocionais dos indivíduos, a partir do emprego da inteligência artificial.

c. Criar normativas e diretrizes que protejam os direitos humanos emergentes, a partir da racionalização dos riscos e impactos sociais na implementação da inteligência artificial, estabelecendo instrumentos proporcionais de prevenção, mitigação e reparações de danos.

d. Estabelecer requisitos de gestão responsável, constituindo para os projetos de IA, os estágios de restrição, suspensão e proibição de aplicações e produtos, em relação aos riscos.

e. Estabelecer o conceito político e jurídico de "excesso*"* nas análises jurisdicionais e na liberação de licenças para negócios modelados com inteligência artificial e internet.

f. Fomentar a construção de normativas regulatórias preventivas, e não somente repressiva, aumentando a velocidade temporal de aplicação do direito, quando houver risco da IA.

g. No plano legislativo, reconstituir o instituto do sigilo industrial, nas aplicações envolvendo IA com a técnica de algorítmos, com foco na transparência e redução da opacidade.

h. Corroborar no plano internacional, pela reformulação da Declaração Universal dos Direitos do Homem, respeitando os direitos emergentes, pensados à luz dos riscos da inteligência artificial, *big data*, geolocalização, algorítmos, reconhecimento facial e uso bélico destas.

i. Aderir ao Tratado de Budapeste para enfrentamento dos crimes cibernéticos, efetivando cooperação internacional para mitigar o fenômeno da extraterritorialidade e ampliar a cibersegurança.

j. Criar expertise, por meio de cooperação internacional sobre neurotecnologia efeitos no sistema cerebral humano, diante dos novos experimentos que envolvem a neurociência, emprego da nanotecnologia no cérebro e inteligência artificial.
k. Colaborar no plano internacional para reformulação dos requisitos da proteção da inviolabilidade civil, a partir da discussão sobre uso das tecnologias no âmbito da guerra, como mísseis nucleares a distância, dronificação da guerra e uso da nanotecnologia.

l. No plano jurídico, definir a *política pública* dos Tribunais Judiciais do Brasil, sobre o emprego da IA nos processos jurídicos, criando medidas de segurança para os dados

compartilhados, definindo prazos e condições de uso destes, bem como, obrigatoriedade de revisor humano nos processos submetidos em camadas contínuas, às aplicações de IA.

m. No plano jurídico, estabelecer modelo de monitoramento dos algorítmos de IA voltados à transparência, em duas etapas distintas: a primeira com foco na auditória, abertura e fiscalização do código-fonte das aplicações do âmbito processual; e na segunda etapa, realizar testes públicos de segurança, para confirmar a integridade dos sistemas e sua correção.

n. No plano processual jurídico, garantir o princípio da inafastabilidade da jurisdição, gerando o direito ao cidadão de discutir uma decisão realizada pelo robô, ou mesmo, *direito ao julgamento humano,* com instrumentos para o cidadão transigir e exigir judicialmente.

o. No plano processual jurídico, garantir o princípio do devido processo legal, definindo a melhor modelagem processual de inteligência artificial, que evite as contínuas instâncias judiciais sem adoção da análise humana em determinadas fases do processo. Considerar que se todas as instâncias implementarem a IA, poderá haver distorções diante da rapidez processual, que podem ser prejudiciais ao direito do cidadão na perspectiva da equidade.

p. Tornar acessível à sociedade, meio de provocação da jurisdição junto aos Tribunais ordinários e superiores, por pessoas prejudicadas por aplicações de IA no âmbito individual, aplicando o modelo similar ao "*recurso de amparo"* existente na Espanha, que prevê acesso aos tribunais de modo facilitado.

q. Criar, ampliar e informar canais e órgãos públicos para reclames quanto ao excesso e abuso, no uso das aplicações de inteligência artificial ou da ocorrência de crimes cibernéticos.

r. Estabelecer como parâmetro de desenvolvimento tecnológico a limitação-regulação da IA, ao contrário da mera proibição, delineando-a para o bem estar e inclusão social, permitindo proibição somente como última ratio, quando os riscos forem demasiados.

s. Exigir educação digital da população com custos para o ente empresarial, na implementação dos projetos de inteligência artificial, visando reduzir a engenharia social.

t. Democratizar o conhecimento sobre funcionamento e transparência da IA aos advogados, defensores, sociedade civil e profissionais de defesa social, informando sobre o planejamento do sistema, representatividade de dados, resultado dos testes de qualidade dos algorítmos e mitigando riscos.

u. Implementar a Lei Geral de Proteção de Dados – *Penal*, visando coibir atuação criminal no ciberespaço e ação das organizações criminosas, visando preencher a lacuna da LGPD (2018), cível, que possui limitações para emprego no âmbito penal e da segurança pública.

v. Proteger o Estado brasileiro, dados sensíveis da população através da atuação conjunta de seus poderes constituídos, reconhecendo a hipossuficiência da sociedade, diante dos negócios empresariais e Estados internacionais; portanto, proibindo a quebra da privacidade, geolocalização e compartilhamento de dados dos cidadãos, com poder de sanção.

w. No âmbito empresarial, determinar permanente monitoramento da inteligência artificial, com proibição da atuação autônoma de máquina, sem fiscalização humana, construindo

modelos de autorregulação empresarial associados à regulação estatal, para redução da opacidade do sistema e substituição de algorítmos discriminatórios, quando houver.

x. Estabelecer níveis de prevenção de riscos de IA e boas práticas organizacionais, com criação de selo de qualidade nos moldes da organização internacional para padronização "*international organization for standardization*" (ISO 9000*)* de gestão ambiental, social e de governança "*environmental, social and governance"* (ESG).

y. Submeter os entes empresariais e estatais, à fiscalização e auditoria de IA por comissão técnica multidisciplinar constituída por instituições como a Defensoria Pública (*amicus vulnerabilis)*, Ordem dos Advogados do Brasil, Polícia Federal, Ministério Público, sociedade civil, entidades especializadas (*amicus curiae*), universidades e institutos através de seus pesquisadores, criando um observatório nacional de IA, com foco na curadoria dos direitos coletivos e humanitários da sociedade.

z. Criar o Poder público comissão técnica multidisciplinar para cooperação internacional para avaliar, monitorar e regular os impactos da inteligência artificial, analisando a neurociência e considerando o neurodireito *ou "neurolaw"*, visando discutir os riscos da intervenção neural e a tutela da capacidade cognitiva das pessoas diante da neurotecnologia, criando um observatório internacional permanente de IA, que se coadune com a iniciativa nacional.

aa. Reconhecer juridicamente de modo expresso na normativa brasileira, a *inviolabilidade neural* e autonomia decisória, prevenindo a cooptação da capacidade cognitiva do ser humano pela neurotecnologia, com foco especial, nos tratamentos medicinais.

bb. Financiar pesquisas no âmbito universitário público sobre Direito Digital, para construção de arcabouço científico sobre inteligência artificial, algorítmos e tecnologias disruptivas, de modo a tornar-se líder da discussão na América Latina e no plano global.

cc.Construir arcabouço regulatório de inteligência artificial e direitos humanos emergentes, modelados a partir do *conhecimento epistemológico-científico multicultural*, ou seja, que privilegie as preocupações dos grupos historicamente excluídos das decisões, como negros, índios, mulheres, grupo LGBTQIA+ e idosos, de modo a produzir regulação robusta que considere as desigualdades brasileiras, indo além, dos atuais modelos eurocêntricos.

dd. Fomentar parcerias público-privada ou utilizar escolas federais e estaduais públicas, para criação de *softwares* de segurança digital, que promovam proteção da população na internet e possa se estabelecer como novo modelo de negócio, voltado à exportação de cibersegurança para a América Latina por meio da cooperação internacional Mercosul, gerando ao mesmo tempo, segurança cibernética à sociedade, e *royalties*, pelo produto genuinamente brasileiro de propriedade intelectual.

REFERÊNCIAS

1. LEGISLAÇÕES

BRASIL. Comando do Exército. Portaria nº. 666, de 4 de agosto de 2010. **Cria o Centro de Defesa Cibernética do Exército e dá outras providências**. *Boletim do Exército*, n. 31, de 6 de agosto de 2010.

BRASIL. Decreto-Lei nº 13.979 de 06 de Fevereiro de 2020. **Decreta Estado de Emergência relativo à Pandemia do Sars Covid-19.**

BRASIL. **Glossário das Forças Armadas.** (MD35-G-01). 4. ed. Brasília, DF: Publicação do Ministério da Defesa, 2007.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. **Dispõe sobre a tipificação criminal de delitos informáticos.** (Lei Carolina Dieckman). Disponível em http://www.planalto.gov.br /ccivil _03/_ato2011-2014/2012/ lei/l12737.htm. Acesso 15 Mai. 2021.

BRASIL. **Projeto de Lei nº 21.** 2021. Disponível em https://www.camara.leg.br /proposicoesWeb/prop_mostrarintegra?codteor= 2129459. Acesso em 30 Set. 2022.

CEPEJ. **Carta europeia de ética**: sobre o uso da inteligência artificial em sistemas judiciais e seu ambiente. 31.ª reunião plenária. Estrasburgo, 3 de dezembro de 2018. (Comissão Europeia para a eficácia da Justiça). Disponível em https://rm.coe.int/carta-etica-traduzida-para-portugues-revista/168093b7e0. Acesso em 15 out. 2022.

CERT.BR. **Regulamento nº 2.350.** (Grupo de Resposta a Incidentes de Segurança para a Internet no Brasil). Comitê Gestor da Internet no Brasil. Disponível em (https://cert.br/sobre/. Acesso em 31 Dez. 2021.

CNJ. **Resolução no 332, de 21 de agosto de 2020**. Conselho Nacional de Justiça (Dispõe sobre a ética, a transparência e a governança na produção e no uso de Inteligência Artificial no Poder Judiciário), 2020. Disponível em https://atos.cnj.jus.br/files/original 191707202008255f4563b35f8e8.pdf. Acesso em 25 Abr. 2022.

CRFB. **Constituição da República Federativa do Brasil de 1988**. Disponível em https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm Acesso em 24 Out.2022.

ESPANHA. ***Ley Orgánica 3/2018, de 5 de diciembre de Protección de Datos Personales y garantía de derechos digitales.*** Boletín Oficial del Estado (BOE) Madrid. Boletín n. 294.p.119800. Disponível em http: //www.boe.es>buscar/act. docphp?id=BOE-A-2018-16673

LGPD. **Lei Geral de Proteção de Dados**. Lei nº 13.709 de 14 de agosto de 2018. Disponível em planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 24 Abr 2022.

OECD. ***Recommendation of the Council on Artificial Intelligence***. (OCDE). 2019(a). Disponível em https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.Acesso 07 out. 2022.

OECD. ***Recommendation on Responsible Innovation in Neurotechnology***. (Recomendação da OCDE sobre inovação responsável em neurotecnologia). 2019(b). Disponível em https://www.oecd.org/science/recommendation-on-responsible-innovationinneurotechnology. htm. Acesso em 12 Nov. 2022.

ONU Brasil. **Declaração Universal dos Direitos Humanos**. (Organização das Nações Unidas) 18 Out. 2022. Disponível em https://brasil.un.org/pt-br/91601-declaracao-universal-dos-direitos-humanos. Acesso em 18 out. 2022(a)

RGPD. **Regulamento (UE) nº 679 do Parlamento Europeu e do Conselho de 27 de abril de 2016.** Regula o tratamento e a livre circulação de dados sensíveis para a proteção de dados das pessoas físicas. Jornal Oficial da União Europeia. Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679 Acesso 11 Nov.2022.

SENADO FEDERAL. **Direitos Humanos: atos internacionais e normas correlatas**. 4ªed. Brasília:Senado Federal, Coordenação de Edições Técnicas, 2013.

TSE. Resolução nº 23.714, de 20 de outubro de 2022.(do Tribunal Superior Eleitoral). **Dispõe sobre o enfrentamento à desinformação que atinja a integridade do processo eleitoral**. Disponível em https://www.tse.jus.br/legislacao/compilada/res/2022/resolucao-no-23-714-de-20-de-outubro-de-2022. Acesso em 20 out. 2022.

2. LIVES E WEBINARES

BELLOSO Martin, Nuria. ***Inteligencia Artificial y derechos digitales****:¿Conveniencia de revisar la Declaración Universal de Derechos Humanos Emergentes*? 07 Abr 2022. vídeo (1h42min28seg.) [Live]. Professora da Universidade de Burgos, Espanha. Realização Observatório Cyber Leviathan e COSMOius. Ciclo de estudos continuados direito e cidadania. Apoio CNPQ [et. al.] Disponível em https://youtu.be/CVjgoFyZHLY.

FRAZÃO, Ana. **Discriminação Algorítmica**. 15 Dez. 2021. vídeo (1h23min27seg.). [Live]. Professora associada da Universidade de Brasília, Brasil. Realização Observatório Cyber Leviathan e COSMOius. Ciclo de estudos continuados direito e cidadania. Apoio CNPQ [et. al.]. Disponível em https://youtu.be/I4i-TYvqQHc.

HARTMANN PEIXOTO, Fabiano. **Inteligência Artificial e Direito:** visão ética e estratégica. 20 out. 2021. vídeo (1h30min25seg.) [Live]. Professor da Universidade de Brasília, Brasil. Realização Observatório Cyber Leviathan e COSMOius. Ciclo de estudos continuados direito e cidadania. Apoio CNPQ [et.al.] Disponível em https://youtu.be/HR3wfOl4bCk.

ROVER, Aires José. **Inovação no direito:** dos algoritmos e seus limites. 09 Dez. 2021. vídeo (1h39min15seg.) [Live]. Professor associado da Universidade Federal de Santa Catarina, Brasil. Realização Observatório Cyber Leviathan e COSMOius. Ciclo de estudos continuados direito e cidadania. Apoio CNPQ [et.al.]. Disponível em https://youtu.be/WbgjjTJ66bo.

RUÍZ, Juana María Gil. ***El paradigma de la ciência jurídica en uma sociedad digital global***. 18 Mai. 2022. Vídeo (1h22min26seg.). [Live]. Professora da Universidade de Granada, Espanha. Realização Observatório Cyber Leviathan e COSMOius. Ciclo de estudos continuados direito e cidadania. Apoio CNPQ [et.al.].Disponível em https://youtu.be/bEEe_c61oPM.

RUSCHI, Filippo. ***Diritto, Guerra e Tecnologia nell'etá dei droni***. 07 Out. 2022. Vídeo (1h34min47seg.). [Live]. Professor da Universidade de Florença, Itália. Realização Observatório Cyber Leviathan e COSMOius. Ciclo de estudos continuados direito e cidadania. Apoio CNPQ [et. al.] Disponível em https://youtu.be/UNpqONOJM-w.

SILVEIRA, Alessandra. **Constitucionalismo Digital:** a distância, o tempo e a linguagem do direito diante da inteligência artificial ubíqua. 21 Jul. 2022. vídeo (1h28min54seg.). [Live]. Professora agregada da Universidade do Minho, Portugal. Realização Observatório Cyber Leviathan e COSMOius. Ciclo de estudos continuados direito e cidadania. Apoio CNPQ [et. al.]. Disponível em https://youtu.be/jdMfdAwyahE.

3. OBRAS PRINCIPAIS

ADEODATO, João Maurício Leitão. **O problema ético: como separar o bom do mau direito.** Revista Jurídica da Presidência. Brasília, v.23 n.130. Jun./Set. 2021. pp.341-366. Disponível em http://dx.doi.org/10.20499/2236-3645.RJP2021V23E130-2191. Acesso em 08 jul. 2022.

ALEXY, Robert. **Teoria dos direitos fundamentais.** Tradução Virgílio Afonso da Silva (da 5ª edição alemã. "*Theorie der Grundrechte" (Fraukfurt am Main: Suhrkam*p, 2006). Malheiros Editores. Capítulos 1 a 3, 2008. pp.1-179 (Coleção teoria & direito público)

ALLCOTT, H.; GENTZKOW, M.. ***Social Media and Fake News in the 2016 Election***. (*Relatório: redes sociais e notícias falsas nas eleições de 2016*). Bureau Nacional de Pesquisa Econômica. *Journal of Economic Perspectives*. Vol31, nº2. Spring, 2017. 118p. Disponível em https://pubs.aeaweb.org/doi/pdfplus /10.1257/jep.31.2.211 Acesso em 22 Mai. 2022.

AMARAL, Camila. **Você conhece todos os robôs que já operam no judiciário brasileiro?** 27/03/2020. Disponível em https://www.migalhas.com.br/depeso/ 322824/voce-conhece-todos-os-robos-que-ja-operam-no-judiciario-brasileiro. Acesso em 25 Abr. 2022.

ARENDT, Hannah. **A Condição Humana**. 10ª ed. Rj: Forense Universitária, 2002.

ATHENIENSE, Alexandre Rodrigues. **As premissas para alavancar os projetos de inteligência artificial na Justiça brasileira.** II Congresso Internacional de Direito, Governo e Tecnologia. Belo Horizonte: Fórum, 2018, p.158.

AXUR. **Relatório de atividade criminosa online no Brasil: 1º Trimestre.** São Paulo, 2021.

AXUR. **Relatório de atividade criminosa online no Brasil: 4º Trimestre.** São Paulo, 2020.

BARROSO, Luís Roberto. **A dignidade da pessoa humana no direito constitucional contemporâneo:** natureza jurídica, conteúdos mínimos e critérios de aplicação. Versão provisória para debate público. Dezembro de 2010.

BBC news Brasil. **Guerra na Ucrânia: o papel crucial dos drones no conflito**. 25 julho 2022. Disponível em https://www.bbc.com/portuguese/internacional-62291582. Acesso em 17 out.2022.

BID. A **inteligência artificial a serviço do bem social na América Latina e no Caribe: panorama da região e retrato de doze países**. (Banco Interamericano de Desenvolvimento). Maio de 2020.

BOMFIM, F.; GIMÉNEZ PEREIRA, M. (Org.) **Teoria do Capital Humano no contexto de inteligência artificial.** Ciências Sociais Aplicadas III: diálogos contemporâneos. 3ed. Salvador: Mente Aberta, v. 3, p. 67-82, 2020a.

BOMFIM, F.; GIMÉNEZ PEREIRA, M. **Tecnologia cognitiva (TC), Inteligência Artificial (IA) e Propriedade Intelectual: algumas reflexões**. Revista Mbote, v. 1, p. 1-11, 2020b.

BOSTROM, Nick; YUDKOWSKY, Eliezer. **A ética da inteligência artificial**. (*The ethics of artificial iIntelligence. Cambridge University Press,* 2011). Tradução de Pablo Araújo Batista. Fundamento Revista de Pesquisa em Filosofia v. 1, n. 3, maio-ago. 2011. pp.200-226. Disponível em https://periodicos.ufop.br/fundamento/article/ view /2270/1722. acesso 08 Out 2022

BOYD, Lain. ***How hypersonic missiles work and the unique threats they pose – an aerospace engineer explains***. *(*Como os mísseis hipersônicos funcionam e as ameaças únicas que eles representam - explica um engenheiro aeroespacial). 15.04.2022. Disponível em https://theconversation.com/how-hypersonic-missiles-work-and-the-unique-threats-they-pose-an-aerospace-engineer-explains-180836 . Acesso em 28 Mai. 2022.

BRITO, Edvaldo. **Limites da revisão constitucional**. Editor: Sérgio Antônio Fabris. Porto Alegre, 1993.

BSI. ***BSI warnt vor dem Einsatz von Kaspersky-Virenschutzprodukten***. (BSI adverte contra o uso de produtos de proteção contra vírus da Kaspersky). 15 mar 2022. Disponível em https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse 2022/220315 _Kaspersky-Warnung.html. Acesso em 25 Abr 2022.

BUDAK, C. **O que aconteceu? A disseminação do conteúdo do editor de notícias falsas durante as eleições presidenciais dos EUA de 2016**. 2019, pp.139-150.

CASTELLS, Manuel. **A sociedade em rede .** *In:* A era da informação: economia, sociedade e cultura – volume I). tradução de Roneide Venâncio Majer. 6ª ed. Editora: Paz e Terra, 1 janeiro 2013.

CERF, Vinton; DALAL Yogen; SUNSHINE, Carl. ***Specification of internet transmission control program.*** version December 1974. Disponível em https://tools.ietf.org/pdf/rfc675.pdf Acesso em 15 Set. 2020.

CERT.BR .**Origem de ataques cibernéticos no Brasil. (**Top10 - por país). 2022. Disponível em https://cert.br/stats/incidentes/2020-jan-dec/top-cc.html. Acesso em 28 Abr. 2022.

CHAMAYOU, Grégoire. **Teoria do drone.** Tradução de Célia Euvaldo. São Paulo: Cosac Naify, 2015. pp.210-250.

CUNHA JÚNIOR, Dirley da. **Curso de direito constitucional**. 15ª ed. rev. ampl. e atual. Editora JusPODIVM. (1.408p). 01 de janeiro de 2021. pp. 107-223; 662.

DA SILVA, Nilton Correia. **Inteligência Artificial**. *In:* FRAZÃO; Mullholand (Coord.) Inteligência Artificial e Direito: ética, regulação e responsabilidade. 2ªed. rev.atual e ampl. São Paulo: Thomson Reuters Brasil. p.33-50, 2020.

DONEDA, Danilo. (2006). **Da privacidade à proteção de dados pessoais**. Rio de Janeiro, Renovar. pp.130-145.

ESET. ***Cyber risks driving SMBs: to enterprise solutions***. 11 Nov. 2022, 17p. (Relatório). Disponível em https://www.welivesecurity.com/wpcontent/uploads/2022/11/eset_smb_digital _security_sentiment_report.pdf. Acesso em 12 Nov. 2022.

FBI. ***The Cyber Threat.*** *Federal Bureau of Investigatio*n (tradução livre: A ameaça cibernética). 2022. Disponível em https://www.fbi.gov/investigate/cyber. Acesso em 24 Abr. 2022.

FERRAZ JÚNIOR, Tércio Sampaio. C**onstituição de 1988:** legitimidade, vigência e eficácia, supremacia. São Paulo: Atlas, 1989.

FERRAZ JÚNIOR, Tércio Sampaio. **Interpretação e estudos da constituição de 1988:** aplicabilidade; congelamento; coisa julgada fiscal; capacidade contributiva; ICMS; e mpresa brasileira; poder constituinte estadual; medidas provisórias; justiça e segurança; servidor público. São Paulo: Atlas, 1990.

FGV. **Relatório da Conferência latino-americana de inteligência artificial e proteção de dados**. (Fundação Getúlio Vargas). 22/10/2021. Disponível em https://www.direitorio.fgv.br/noticia/relatorio-conferencia-latino-americana-de-inteligencia-artificial-e-protecao-de-dados. Acesso em 24 Abr. 2022.

FRAZÃO, Ana. **Discriminação algorítmica:** por que algoritmos preocupam quando acertam e erram? mapeando algumas das principais discriminações algorítmicas já identificadas. 2021. Disponível em https://www. jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-

mercado/discriminacao-algoritmica-por-quealgoritmos-preocupam-quando-acertam-e-erram-0408202. Acesso em 12 out. 2022.

FRAZÃO, Ana. ***Geopricing e geoblocking*:** as novas formas de discriminação de consumidores. Os desafios para o seu enfrentamento. 2018. Disponível em https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/ ge opricing-e-geoblocking-as-novas-formas-de-discriminacao-de-consumidores15082018. Acesso em 08 out. 2022.

FROSINI, Vittorio. ***L'uomo artificiale:*** *etiica e diritto nell'era planetaria*. Milano: Spirali Edizione, 1986.

GROSFOGUEL, Ramón. **A estrutura do conhecimento nas universidades ocidentalizadas:** racismo/sexismo epistêmico e os quatro genocídios/epistemicídios do longo século XVI. Revista Sociedade e Estado. vol. 31, n. 1 Janeiro/Abril, 2016. pp.25-49. Disponível em https://www.scielo.br/j/se/a/XPNFtGdzw4F3dpF6yZVVGgt/?format =pdf&lang=PT. Acesso em 08 Out. 2022.

HARTMANN Peixoto, Fabiano. **Direito e Inteligência Artificial**. Brasília, 2020. (Coleção Inteligência Artificial e Jurisdição, vol. 2). [livro digital]. Disponível em https://livros.unb.br/ index.php/portal/catalog/book/200. Acesso em 14 Set. 2022.

HARTMANN, Ivar A. (Coord.) **Regulação de inteligência artificial no Brasil: *policy paper***. Fundação Getulio Vargas (FGV Direito Rio) 2020. Disponível em https://bibliotecadigital.fgv.br/dspace;handle/handle/10438/30078. Acesso 07 Out. 2022.

HARVARD Business Review Analytic Services. ***Aligning Your Entire Organization Around the Customer***. *(Alinhando toda a sua organização em torno do cliente*) Quantum Metric. 11p. Disponível em https://hbr.org/resources/pdfs/comm/Quantum%20Metric/AligningYourEntire OrganizationAroundtheCustomer.pdf. Acesso em 15 Abr. 2022.

IBM. Relatório de IBM Security: **Dobram os ataques às indústrias que dão suporte aos esforços em resposta à COVID-19.** Cambridge, 24 de fevereiro de 2021. Disponível em https://www.ibm.com/blogs/ibm-comunica/ibm-security-ataques-ciberneticos/. Acesso em 30 Mar. 2022.

IHERING. Rudolf Von. **A luta pelo direito.** (Tradução Edson Bini). 2ª ed. São Paulo: Edipro, 2019.

INTERPOL. ***Ciberdelincuencia: efectos de La Covid-19***. França, AGO/2020. 20p. Disponível em http://www.interpol.int. Acesso em 20 Out. 2020.

INTERPOL. ***Estratégia Mundial contra La ciberdelincuencia:*** *resume.n* França, agosto de 2020. Disponível em http://www.interpol.int. Acesso em 20 Out. 2020.

JOHNS HOPKINS University. ***Coronavirus resource center***. Disponível em https://coronavirus.jhu.edu/map.html. Acesso em 23 out. 2022.

JOHNSON, David Reynold; POST, David G. ***Law and Borders - the Rise of Law in Cyberspace.*** Stanford Law Review, Vol. 48, 1996. 1367p. Disponível em https://ssrn.com/abstract=535 or http://dx.doi.org/10.2139/ssrn.535**. A**cesso em 30 Dez. 2021.

JOSE, X; KUMAR e CHANDRAN, P. ***Characterization, Classification and Detection of Fake News in Online Social Media Networks***. *(Caracterização, classificação e detecção de fake news em redes sociais online). IEEE Mysore Sub Section International Conference*,2021. pp. 759-765. Doi: 10.1109/MysuruCon52639.2021. 9641517. Acesso em 22 Mai. 2022.

KAHN, Robert; CERF, Vinton. ***A protocol for packet network interconect***. 1974.

KASPERSKY *Security Network.* **América Latina registra 3,7 milhões de ataques de malware por dia**. 2018. Disponível em https://www.kaspersky.com.br/blog/america-latina-37-milhoes-ataques-malware-dia/11151/. Acesso em 25 Out. 2020**.**

KASPERSKY *Security Network.* **O que é cibersegurança?** Disponível em https://www.kaspersky.com.br/resource-center/definitions/what-is-cyber-security. Acesso em 25 Out. 2020**.**

KASPERSKY. **Danos colaterais na cibersegurança:** carta aberta de Eugene Kaspersky em resposta ao aviso contra o uso de produtos Kaspersky pelo Escritório Federal Alemão de Segurança da Informação (BSI). 17 mar 2022. Disponível em https://www.kaspersky.com.br/blog/collateral-damage-on-cybersecu rity/19103/. Acesso em 25 Abr. 2022.

LEITE DA SILVA, Júlio Cezar Barreto. **Guerra cibernética: a guerra no quinto domínio, conceituação e princípios**. Esc Guerra Naval, Rio de Janeiro, v. 20, n. 1, p. 193-210, jan./jun. 2014.

LÉVY, Pierre. **O que é virtual? (**Tradução de Paulo Neves). São Paulo, Editora:34, 1996. 157p. (Coleção Trans)

LIN, Herb. ***Cybersecurity Lessons from the Pandemic, or Pandemic Lessons from Cybersecurity.*** June 2, 2020. Disponível em https://www.lawfareblog. com/cybersecurity-lessons-pandemicor- pandemic-lessons-cybersecurity. Acesso em 15 Ago. 2020**.**

LLINARES, Fernando Miró. ***Policia predictiva: utopia o distopia?*** *Sobre les actituds cap a l'ús d'algorismes de big data per a l'aplicació de la llei. IDP: revista d'Internet, dret i política.* nº 30, 2020.

MAIA FILHO, Mamede Said e JUNQUILHO, Tainá Aguiar. **Projeto Victor: perspectivas de aplicação da inteligência artificial ao direito**. R. Dir. Gar. Fund., Vitória, v. 19, n. 3, p. 219-238, set./dez. 2018.

MARCEL, Leonardi. **Fundamentos do Direito Digital**. [livro digital]. Editora: Revista dos Tribunais. 2019, 400p.

MCAFEE, Labs. ***Threats Report*** (*Relatório de ameaças*). April 2021. Disponível em https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-apr-2021.pdf acesso em 25 Mai. 2021.

MCAFEE. ***The hidden costs of cybercrime***.(Tradução livre: Os custos ocultos do crime cibernético). 07 December 2020. Disponível em https://www.mcafee.com/enter prise/pt-br/about/newsroom.html. Acesso em 15 Jan. 2022.

FERRER, Salvador Morales. ***La actuación de la ley de protección de datos española y el reglamento europeo:*** *un estudio sobre su aplicación en el derecho a la información y el consentimiento informado, datos clínicos y documentos hospitalarios de ló s médicos y pacientes en españa*. Revista de Direito Brasileira. Florianópolis, v. 23, n. 9, 2019. p. 268-283 Disponível em: https://blook.pt/publications/publication/92b3d9373fd9/ Acesso 22 Nov. 2022

FERRER, Salvador Morales. ***La protección de datos personales em lós asistentes digitales como Siri o Alexa***. In: BARBOSA, Mafalda M. [et. al.]. Direito digital e inteligência artificial: diálogos entre Brasil e Europa (1.136p). Editora Foco, 2021. pp. 289-305.

MULHOLLAND, Caitlin. Responsabilidade **civil e processos decisórios autônomos em sistemas de Inteligência Artificial (IA):** autônoma, imputabilidade e responsabilidade. *In:* Inteligência Artificial e Direito: ética, regulação e responsabilidade. (MULHOLLAND & FRAZÃO- coord.). 2ª ed. rev. atual. ampl. São Paulo: Thomson Reuters, 2020. pp.327-348.

OLIVEIRA, Clara Costa. **Da cibernética à autopoiesis:**continuidades e descontinuidades**.** Revista informática na educação: teoria & prática. Porto Alegre, v.12, n.2, jul./dez. 2009. pp.23-34.

ONU Brasil. **Como as Nações Unidas apoiam os objetivos de desenvolvimento sustentável no Brasil**. Disponível em https://brasil.un.org/pt-br/sdgs. Acesso em:20 out. 2022b.

PARKS, R.C. DUGGAN, D.P. ***Principles of Cyberwarefare***. 2001. I*n: IEEE Security & Privacy*, v. 9, n. 5, p. 30-35, Sept./Oct. 2011.

PERRIN, Stephanie. **O cibercrime.** *In:* Desafios de Palavras: enfoques multiculturais sobre as sociedades da informação. (AMBROSI, Alain, PEUGEOT, Valérie e PIMIENTA, Daniel. Coords) C&F Éditions. 2005.

PROVOST, F. ***Data science for business:*** *what you need to know about data mining and data - analytic thinking*. (Ciência de dados para negócios: o que você precisa saber sobre mineração de dados e dados - pensamento analítico). O'Reilly Media, 2013.

PROVOST, F; FAWCETT, T**.** ***Data science and its relationship to big data and data-driven decision making.*** (Ciência de dados e sua relação com *big data* e tomada de decisão orientada por dados.) 2013.

RAMÍREZ, Manuel Becerra. ***El capitalismo del conocimiento y la propiedad intelectual.*** *I*n: Bergel, Salvador D y Negro, Sandra. *Propiedad intelectual,Presente y Futuro.* Editorial: IB de IF. Buenos Aires, 2019. pp.1-18.

RAMOS, Silvia (Coord.). **Retratos da Violência** – Cinco meses de monitoramento, análises e descobertas. Rio de Janeiro: Rede de Observatórios da Segurança/CESeC, 2019.Disponível em http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca /bibli_servicos_produtos/BibliotecaDigital/BibDigitalLivros/TodosOsLivros/Retratos-da-violencia%3Dcinco-meses-de-monitoramento.pdf. Acesso em 07 Dez. 2022

SAMPAIO, Fernando G. **Ciberguerra, guerra eletrônica e informacional: um novo desafio estratégico.** Porto Alegre: Escola Superior de Geopolítica e Estratégia, 2001. Disponível em http://www.defesanet.com.br/esge/ciberguerra. pdf. fls 3-4. Acesso em 12 Mai. 2022.

SCHWAB, Klaus. **A quarta revolução industrial**. Edipro, 2019.

SENADO DOS ESTADOS UNIDOS**.** S.HRG. 115-683 - ***Facebook, social media privacy, and the use and abuse of data.*** (Comissões do Judiciário e do Comércio, Ciência e Transporte do Senado dos Estados Unidos). Segunda Sessão, nº de série J–115–40, 10 Abr 2018. Disponível em https://www.congress.gov/115/chrg/CHRG-115shrg37801/CHRG-115shrg37801.pdf. Acesso em 12 Abr. 2020.

SHAPIRO, Aaron. ***Predictive policing for reform****? Indeterminacy and intervention in big data policing.* Surveillance & Society, v. 17, n. 3/4, 2019. págs. 456-548.

SILVA, Edna Lúcia da; MENEZES, Estera Muszkat. **Metodologia da Pesquisa e Elaboração de Dissertação**. 4ª ed. rev. Atual. Universidade Federal de Santa Catarina – UFSC. Florianópolis, 2005. 140p.

SILVA, Tarcízio. **Linha do Tempo do Racismo Algorítmico**. Blog do Tarcízio Silva, 2019. Disponível em: https://tarciziosilva.com.br/blog/posts/racismo-algoritmico-linha-do-tempo. Acesso em: 08 Out. 2022.

SILVA, Tarcízio. **Racismo Algorítmico:** inteligência artificial e discriminação nas redes digitais. São Paulo: Edições Sesc, 2022. pp. 01- 56.[livro digital]

SOARES, Ricardo Maurício Freire. **O discurso constitucional da dignidade da pessoa humana:** uma proposta de concretizaçâo do direitojusto no pós-positivismo brasileiro. (Tese) Programa de Pós- Graduação em Direito. Universidade Federal da Bahia, 2008. 276p.

SOPHOS. ***The State of Ransomware 2022***. (O estado do Ransomware 2022- Relatório) https://assets.sophos.com/X24WTUEQ/at/4zpw59pnkpxxnhfhgj9bxgj9/sophos-state-of-ransomware-2022-wp.pdf Disponível em 12 Nov. 2022.

SUAREZ; ACÁCIO. **Terrorismo de baixo custo ou a ameaça invisível:** o terrorismo e as políticas brasileiras de antiterrorismo. Austral: Revista Brasileira de Estratégia e Relações Internacionais, v.7, n.14, Jul./Dez. 2018. p.92-111.

SUPREMO Tribunal Federal. **STF valida compartilhamento de dados mediante requisitos.** 15 set. 2022. Disponível em https://portal.stf.jus.br/noticias/verNoticia Detalhe.asp? idConteudo=494227&ori=1. Acesso em 16 set. 2022.

TAUHATA; MOREIRA. **E-mails maliciosos subiram 600% em março, após alta do home office, diz IBM.** Valor Econômico. São Paulo. 10/06/2020 - 13h58. Disponível em https://www.ibm.com/blogs/ibm-comunica/module/cybersecurity/. Acesso em 15 Jul. 2021.

TJBA. **TJ-BA e TJ-SP discutem uso de inteligência artificial e automatização em processos.** (Tribunal de Justiça da Bahia). 15 Out. 2022. Disponível em http://www5.tjba.jus.br/portal/tribunais-de-justica-da-bahia-e-de-sao-paulo-discutem-uso-de-inteligencia-artificial-e-automatizacao-em-processos-judiciais/ Acesso em 12 Nov. 2022.

TREND Micro Research. ***Attacks From All Angles:*** *2021 Midyear Cybersecurity Report*. Disponível em https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/attacks-from-all-angles2021-midyear-security-roundup.Acesso em 15 Abr. 2022.

TREND Micro Research. **Em direção a um novo momento:** previsões de Trend Micro Security para 2022. Disponível em https://documents.trendmicro.com/assets/rpt/rpt-BR-toward-a-new-momentum-trend-micro-security-predictions-for-2022.pdf.Acesso 15 Abr. 2022.

TURING, Alan. ***Computing Machinery and Intelligence***. Mind.1950. Disponível em http://doi:10.1093/mind/LIX.236.433. Acesso em 20 Abr. 2020.

WADSWORTH, Christina; VERA, Francesca; PIECH, Chris. ***Achieving fairness through adversarial learning: an application to recidivism prediction***.(*Alcançando a justiça por meio do aprendizado contraditório: uma aplicação para previsão de reincidência*). Disponível em https://arxiv.org/abs/1807.00199 2018. Acesso em Jul. 2021.

WENDT, Emerson. **Ciberguerra, inteligência cibernética e segurança virtual: alguns aspectos**. Revista Brasileira de Inteligência. Brasília: Abin, n. 6, abr. 2011.

WIENER, Norbert. ***Cybernetics: or the control and communication in the animal and the Machine***. *(Cibernética: ou o controle e a comunicação no animal e na máquina)* 2ª ed.

Cambridge, Massachusetts, 1948. pp. 144-168. Disponível em https://uberty.org/wp-content/uploads/2015/07/Norbert_Wiener_Cybernetics.pdf. Acesso em Abr. 2022.

XAVIER, P.; PORTALÉS, S.; GUIMARÃES, T. & FARIAS, K. **Polícia preditiva e "negritude":** modelos para a reprodução de um estado sem direitos. *In: Seguridad y los retos de la jurisdicción en el siglo XXI: justicia,sostenibilidad y paz.*Editora Colex. 2022, pp.27-54.

XAVIER, P.R.S. ***La transformación digital de justicia: viejos paradigmas, nuevos horizontes.***1ª ed. Málaga, Espanha: Editorial Colex. 24 fevereriro 2021, 286p. [livro digital]

XAVIER, P.R.S. ***Gobernanza, Inteligencia Artificial y Justicia Predictiva:*** *los retos de la Administración de Justicia ante la sociedad en red*. (Tese doutoral).Universidad de Málaga. Espanha, 2020.

YUSTE, R. & BARGMANN, C. ***Toward a Global BRAIN Initiative***. *(Rumo a uma Iniciativa Global BRAIN).* vol.168, n.6. 2017, pp. 956-959. Disponível em https://www.sciencedirect. com/science/article/pii/S009 2867417302015. Acesso em 05 Set. 2022.

YUSTE, R., GOERING, S., ARCAS, B. (*et.al.)* ***Four ethical priorities for neurotechnologies and AI. Nature***. *(Quatro prioridades éticas para neurotecnologias e IA)* n.551,2017b.pp.159-163. Disponível em https://doi.org/10.1038/551159a. Acesso 05 Set. 2022.

YUSTE, R; GOERING, S.; (*et al).* ***Recommendations for Responsible Development and Application of Neurotechnologies.*** (*Recomendações para Desenvolvimento Responsável e Aplicação de Neurotecnologias*) *Neuroethics* 14, 365-386. 2021. Disponível em https://doi.org/10.1007/s12152-021-09468-6. Acesso em 10 Nov. 2022.

4.OBRAS CONSULTADAS

ASSAF NETO, Alexandre. **Mercado financeiro**. São Paulo: Atlas, 2015. p.158

BELLOSO Martin, Nuria. ***Algunos efectos perversos de la globalización****: las empresas transnacionales y el deber de respeto de los estándares mínimos internacionales de derechos humanos.* Cuadernos Electrónicos de Filosofía del Derecho, n. 28, 2013. 35p.

BOGARD, William. ***Simulation and pos-panopticism***. In BALL, Kirstie; LYON, David; HAGGERTY, Kevin D. (Ed**.).** *Routledge handbook of surveillance studies*. Routledge, 2012. p. 30.

BURKE-White, William W.; SLAUGHTER, Anne-Marie. ***An International Constitutional Moment.*** *Harward Internacional Law Journal* I, volume 43, 2002.

CÂMARA DEPUTADOS. **Debatedores defendem regulação setorial para uso de inteligência artificial no Brasil**. 10/08/2021 Disponível em https://www.camara.leg.br/ noticias/792088-debatedores-defendem-regulacao-setorial-para-uso-de-inteligencia-artificial-no-brasil/ Acesso em 25 Abr. 2022.

CÂMARA DEPUTADOS. **Projeto cria marco legal para uso de inteligência artificial no Brasil**. 04/03/2020. Disponível em https://www.camara.leg.br/noticias/641927-projeto-cria-marco-legal-para-uso-de-inteligencia-artificial-no-brasil Acesso em 25 Abr. 2022.

CAVALCANTE, Andréa de Fátima Araújo. **A atipicidade dos crimes cibernéticos no Brasil e a impunidade:** uma análise crítica**.** Disponível em http://repositorio.

favip.edu.br:8080/bitstream/123456789/866/1/Monografia+Andrea+de+F%C3%A1tima+Ara%C3%BAjo+Cavalcante.pdf. Acesso em 13 Jul. 2020.

CISO ADVISOR. **300 mil hackers alistados para atacar pela Ucrânia.** 16 Mar. 2022. Disponível em https://www.cisoadvisor.com.br/300-mil-hackers-na-guerra-cibernetica -pela-ucrania/. Acesso em 10 Mai. 2022a.

CISO ADVISOR. **E-commerce sofreu 162 milhões de ataques nos últimos 18 meses:** Levantamento mostra que este foi o número ciberataques aos e-commerces brasileiros entre abril de 2021 e setembro deste ano. 2022. Disponível em https://www.cisoadvisor.com.br/e-commerces-sofreram-162-milhoes-de-ataques-nos-ultimos-18-meses/.Acesso em 12 Nov. 2022b.

CORRIERE della Sierra. ***202 secondi per incenerire Londra con un'atomica»: la simulazione alla tv russa:*** *Il Primo canale russo ha mostrato una simulazione della distruzione che le armi atomiche potrebbero causare sulle città europee.* Disponível em https://www.corriere.it/Esteri/22_aprile_30/tv-russa-bomba-atomica-londra-parigi-berlino-908382e4-c86e-11ec-85c4-7c8d22958d02.shtml. Acesso em 30 Abr. 2022.

DE SOUZA, Paulo Vinicius Sporleder. **Biobancos, dados genéticos e proteção jurídico-penal da intimidade**". *Revista AMRIGS*, n. 56 (3), jul-set 2012, pág. 268-273

DEFESA NET. **China confirma *cyber blue team*.** Maio/2011. Seção Tecnologia. Disponível em: <http://www.defesanet.com.br/tecnologia/noticia/1167/China-confirma—Cyber-Blue-Team>. Acesso em 29 Mai. 2022.

DIAS, Sérgio Vidal dos Santos. **Auditoria de processos organizacionais**. São Paulo: Atlas, 2008. p.23

EVERIS. **Relatório sobre o impacto da Inteligência Artificial (IA) no empreendedorismo da América Latina**. Disponível em https://www.everisestudos.com.br/estudo-inteligencia-artificial Acesso em 25 Abr. 2022.

FERGUSON, Andrew G. ***Policing Predictive Policing***. *Wasington University Law Review*, n.º 94. Whashington, 2017. p.1109. Disponível em https://openscholarship.wustl.edu/law_lawreview/vol94/iss5/5. Acesso em 10 Jan. 2021.

FIOCRUZ. **O que é uma pandemia?** (Fundação Oswaldo Cruz). 14 Out 2020. Disponível em HTTPS://www.bio.fiocruz.br/índex.php/bt/noticias/1763-o-que-e-uma-pandemia. Acesso 15 Mar. 2021.

GOLDIM, José Roberto. **Conferência de Asilomar**. 1997. Disponível em https://www.ufrgs.br/bioetica/asilomar.htm. Acesso 08 out. 2022

JBS. ***JBS-USA cyberattack media statement.*** 2021. Disponível em http://jbsfoodsgroup.com/articles/jbs-usa-cyberattack-media-statement-may-31.Acesso 20 Fev. 2022.

JBS. **Ransomware segue gerando caos na indústria e jbs se pronuncia sobre ciberataque**. 2021. Disponível em https://www.securityreport.com.br/destaques/ransomware-segue-gerando-caos-na-industria-e-jbs-se-pronuncia-obreciberataque/#.YZ2PGFXMLIX. Acesso em 20 Fev. 2022.

KAHNEMAN, Daniel; SIBONY, Olivier; SUNSTEIN, Cass. R. **Ruído: uma falha no julgamento humano.** (Tradução de Cássio de Arantes Leite). Editora Objetiva. 2021, 432p.

KOLAKOWSKI, Mark. ***Facebook (fb) whistleblower testifies before us Senate: Calls Facebook 'morally bankrupt' and undeserving of 'blind trust'***. (*Denunciante do Facebook*

(fb) testemunha perante o Senado: chama o Facebook de 'moralmente falido' e indigno de 'confiança cega'). 05 Out. 2021. Disponível em https://www.investopedia.com/facebook-fb-whistleblower-testifies-before-us-senate5204699. Acesso em 10 Out. 2021.

MITNICK, Kevin D**.** e William L. Simon. **A arte de enganar.** Editora Pearson Education do Brasil Ltda, 2003.

MOORE, Malcolm. Rastreando GhostNet: **investigando uma rede de espionagem cibernética.** *Citizen Lab, Munk Centre for International Studies, University of Toronto*. 2009, 52p.Disponível em https://www.telegraph.co.uk/news/worldnews/asia/china/5071124/Chinas-global-cyber-espionage-network-GhostNet-penetrates-03countries.html. acesso em 20 Mai. 2020.

OCDE. **A caminho da era digital no Brasil**. Paris, 2020. Disponível em https://www.oecd-ilibrary.org/science-and-technology/a-caminho-da-era-digital-no-brasil_45a84b29-pt.Acesso em 22 Jun. 2021.

OLIVE, León. ***Multiculturalismo y derechos humanos***. Fontamara. México, 2014.

PINTO, Paulo Silva. **Inclusão bancária será completa depois de auxílio emergencial, diz presidente da Caixa**. 08 out. 2020. Disponível em https://www.poder360.com.br/governo/inclusão -bancaria-sera-completa-depois-de-auxilio-emergencial-diz-presidente-da-caixa/. Acesso em: 23 out.2022.

PONCE Solé, Juli. ***Inteligencia artificial, Derecho administrativo y reserva de humanidad: algoritmos y procedimiento administrativo debido tecnológico***. Revista General de Derecho Administrativo, n.50. Editorial Iustel. Madrid. 2019, p.2.

SIMAS, Diana Viveiros de. **O cibercrime.** 2014. 168f. Dissertação (Mestrado em Ciências Jurídico Forenses). Universidade Lusófona de Humanidades e Tecnologias. Lisboa, 2014.

UNESCO. **Fórum Regional de Inteligência Artificial na América Latina e no Caribe.** Nota conceitual. 2019. Disponível em https://unesco-regional-forum-ai.cetic.br/pt/ Acesso em 24 Abr. 2022.

VILAR, Silvia Barona. ***La sociedad postcoronavirus con big data, algoritmos y vigilancia digital,¿ excusa por motivos sanitarios?,¿ y los derechos dónde quedan?.*** *Revista Boliviana de Derecho* n. 30. 2020. p. 14-39.