VI ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS II

DANIELLE JACON AYRES PINTO

EDSON RICARDO SALEME

FERNANDO GALINDO AYUDA

D597

Direito, governança e novas tecnologias II [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Danielle Jacon Ayres Pinto; Edson Ricardo Saleme; Fernando Galindo Ayuda – Florianópolis; CONPEDI, 2023.

Inclui bibliografia
ISBN: 78-65-5648-746-5
Modo de acesso: www.conpedi.org.br em publicações
Tema: Direito e Políticas Públicas na era digital

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direito. 3. Governança e novas tecnologias. VI Encontro Virtual do CONPEDI (1; 2023; Florianópolis, Brasil).

CDU: 34

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

VI ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS II

Apresentação

Apresentação do CONPEDI – novas tecnologias.

O grupo constituído por DANIELLE JACON AYRES PINTO, FERNANDO GALINDO e EDSON R. SALEME presidiram o GT Direito, Governança e novas tecnologias II, que tiveram o privilégio de conduzir excelentes trabalhos apresentados, que apontaram as necessidades brasileiras mais prementes, em termos normativos, na era digital. Os trabalhos abordaram as características mais marcantes que estão sujeitos os dados, sobretudo em face da LGPD, mediante a apresentação de propostas para a governança democrática. Outros temas a destacar foram os relacionados ao uso de tecnologias da informação e comunicação nos julgados, bem como de que forma os tribunais brasileiros estão empregando programas de inteligência artificial e como se poderia encontrar limites a essa utilização.

O primeiro a apresentar o trabalho foi o doutorando Ronaldo Felix Moreira Junior acerca da disseminação de notícias falsas e os limites do uso de dados pessoais em campanhas eleitorais, que abarcou a LGPD discutindo como os dados pessoais sensíveis têm sido empregados para fins políticos, como instrumentos de ataque à democracia. O discente Lorenzo Borges de Pietro apresentou o trabalho denominado "A (in) constitucionalidade da suspensão de plataformas da internet em decorrência do descumprimento de decisão judicial: um debate a luz do princípio da proporcionalidade, discutindo o alcance das decisões judiciais em termo de internet. O tema entabulado no próximo artigo foi o "Colonialismo Digital e os entraves à proteção de direitos fundamentais na era do Capitalismo de Vigilância", por Ronaldo Felix Moreira Junior, que apresentou o primeiro trabalho. Discutiu-se que os dados pessoais foram incluídos no rol de direitos fundamentais e que grandes empresas, contratadas para lidar com dados pessoais, podem empregá-los a seu talante. Portanto, deve existir uma tecnologia própria para a proteção deles. Pedro Ribeiro Fagundes apresentou o trabalho acerca da importância da gestão de riscos para a motivação dos atos administrativos. Esta motivação, essencial em todo o ato, deve levar em consideração os riscos que o gestor pode incidir, bem como os respectivos prejuízos que esses riscos podem produzir. Tainara Conti Peres e Deise Marcelino da Silva apresentaram o trabalho "A LGPD e a sua adequação no ambiente laboral: sob a ótica de controle do empregador privado brasileiro." As autoras inferem que a proteção de dados é própria desta época e abordaram, especificamente, as relações trabalhistas e analisam como se aplicam nas relações de trabalho, sobretudo sob a óptica do empregador privado. Valdir Rodrigues de Sá e Irineu

Francisco Barreto Júnior, que se encarregaram do tema “Liberdade de expressão nas plataformas digitais”, teve como objeto a análise da prática de crimes com a abertura da liberdade virtual existente no presente. O próximo trabalho apresentado por Gabrieli Santos Lacerda da Silva, dedicou-se ao tema “Os limites do consentimento frente ao direito fundamental de proteção dos dados pessoais”, que abordou a temática da mudança do comportamento humano diante dos avanços digitais. Nesse sentido, o grande volume de dados da internet, entre eles os dados pessoais, geram implicações na própria dinâmica social, o que fez a CF incluir dispositivos constitucionais e infraconstitucionais. Após a apresentação e aluna Tricieli Radaelli Fernandes e Fernando Hoffmam trouxeram a temática “O capital e a(s) guerra(s) na era do capitalismo de vigilância e a constituição de tecnopolíticas de combate”. O trabalho reflete que pode ser uma guerra real ou de violência simbólica diante da existência de tecnologias que podem perpetuar ou resgatar fórmulas capitalistas existentes nas diversas zonas. A seguir passou-se a apresentar por Estella Ananda Neves o artigo “Análise econômica do impacto da inteligência artificial nos tribunais brasileiros.” O baixo nível de investimentos e a parca participação de empresas brasileiras refletem o desenvolvimento atual do país e afirmam que o Judiciário pode em muito auxiliar o aprimoramento do Brasil. O primeiro bloco finalizou com a apresentação do trabalho “Administração Pública na era digital: uma análise sobre a segurança de dados nas sociedades de economia mista e empresas públicas à luz da LGPD” apresentado por Jean Marcel dos Santos. Como proteger os dados no atual panorama. O primeiro bloco foi encerrado com considerações dos coordenadores do GT, sobretudo o Prof. Galindo, que observou a questão da vigilância de dados nos sistemas jurídicos, a exemplo do que se pode observar na legislação europeia, como a que estabelece regras acerca da inteligência artificial, cuja matéria continua sendo regulada pelo Parlamento Europeu que, no último 14 de junho de 2023, aprovou sua posição negociadora sobre a Lei de Inteligencia Artificial. Importante recordar que esta norma incluí, entre os sistemas de alto risco os sistemas de IA que estão referidos na Administração de Justiça.

O segundo bloco de intervenções começou com o trabalho de Roseli Rêgo Santos Cunha Silva abordou no trabalho A LGPD e o tratamento de dados por agentes de pequeno porto: uma análise a partir da Resolução CD/ANPD N°2/2022. A abordagem indica que devem ser disponibilizados meios, compatíveis com as atividades de menor porte, considerando o bem que a LGPD objetiva proteger, a Resolução não exclui atores de menor porte; o discente Guilherme Elias Trevisan apresentou o trabalho “Big tech, dados, infraestruturas digitais e as universidades públicas federais brasileiras.” Restringiu-se a analise da verificação do sigilo da infraestrutura de dados e a disparidade de tecnologia que geram impactos geopolíticos, sobretudo nas universidades federais. Lidiana Costa de Sousa Trovão e Igor Marcellus Araujo Rosa apresentaram o trabalho intitulado “Cidades Inteligentes Sustentáveis,

governança e regulamentação de dados"; o trabalho analisa como essas cidades podem atingir o objetivo socioambiental e a quem são efetivamente destinadas. A seguir Luiz Fernando Mingati passou a expor o trabalho Constitucionalismo na era digital: os desafios impostos pela era informacional frente às garantias constitucionais. O artigo versa sobre como o impacto da era da informação e como ocorrem modificações na ordem interna geradas por esse fato. A seguir o Prof. Lucas Gonçalves da Silva apresentou juntamente com o aluno Reginaldo Felix "Tributação e Novas Tecnologias", os autores indicam que há uma tributação apresenta um novo percalço pela falta de transparência que os entes tributantes possuem diante desta atividade. O próximo trabalho trouxe a temática "Das cortes físicas às cortes digitais: a transformação digital dos tribunais como instrumento de acesso à justiça", pelo aluno Dennys Damião Rodrigues Albino; a temática se concentra na possibilidade de o Judiciário acompanhar a atual tendência digital e quais seriam as condicionantes a essas mudanças. A seguir David Elias Cardoso Camara apresentou o trabalho "Software de decisão automatizada como ferramenta de compliance no Tribunal de Justiça do Maranhão." O artigo estabelece uma análise geral sobre alguns documentos do Banco Mundial que analisa algumas ineficiências do Poder Judiciário. A seguir o aluno Pedro Gabriel C. Passos analisa no artigo "Desafios para concretização do ODS 8: análise a partir da dinâmica da indústria 4.0" que trata das TICs no ambiente do trabalho e alguns fenômenos que este pode apresentar em termos de prestação de serviços no mundo digital. Thiago Leandro Moreno seguiu apresentando o trabalho "Direito e Tecnologia: criptoativos e tokens não fungíveis", o trabalho versa sobre a ideia do metaverso e as transações ocorridas nos espaços virtuais. Novamente Irineu Francisco Barreto Jr e Kelly Cristina Maciel da Silva apresentaram o trabalho "O paradoxo entre a garantia constitucional do direito à informação e a preservação da privacidade em banco de dados públicos e privados." Constata-se pelo artigo que não existe ainda proteção suficiente para eventuais ataques virtuais.

O último bloco iniciou-se com o artigo "Mercosul X União Europeia: necessária adequação da autoridade nacional de proteção de dados" por Bruno Alexander Mauricio e Kennedy Josué Grecca de Mattos. A seguir apresentou-se o artigo "Mitigação de vieses algorítmicos em processos decisórios: os impactos da diversidade na constituição de equipes desenvolvedoras de inteligência artificial", por Airto Chaves Jr e Pollyanna Maria da Silva. O objetivo da investigação é verificar os impactos da constituição de equipes responsáveis pelas inteligências artificiais. Na sequencia José Octávio de Castro Melo apresentou o trabalho "Novas tecnologias e regulação: uma análise do PL 872/2021 face ao dever de diligência do Estado na proteção do direito à privacidade." A apresentação do trabalho "O uso da inteligência artificial no âmbito do processo judicial: desafios e oportunidades" por Jordy Arcadio Ramirez Trejo e Saulo Capelari Junior abordou de que forma deve ser implementada a inteligência artificial no âmbito do Poder Judiciário. A seguir Luciana

Cristina de Souza apresentou o trabalho “Risco no uso das inteligências artificiais e segurança digital” levando em consideração a atual forma que se aborda possíveis culpados com possível transgressão ao principio da presunção de inocência. Na sequência, Thais Aline Mazetto Corazza, expôs o trabalho “Os riscos na tomada de decisões por máquinas”. Já existe, no âmbito dos tribunais, certa triagem para evitar repetições e assim proporcionar melhores benefícios. Deve-se ter cuidado ao aplicar essas ferramentas, pois possuem subjetividades complexas. Bruno Mello Corrêa de Barros Beuron apresentou o trabalho “Revolução tecnológica e sociedade pós-moderna: perspectivas da obsolescência programada e do direito do consumidor à luz da metateoria do direito fraterno” . Luciana Rodrigues dos Santos e Aparecida Moreira de Oliveira Paiva apresentaram o artigo “Risco no uso das inteligências artificiais e segurança digital” em que se observa a questão relacionada a inteligência artificial pelos órgãos públicos e as questões discriminatórias.

Ao final houve manifestação de todos relativamente ao conteúdo apresentado e o quanto enriquecedor o Grupo de Trabalho foi para todos com ponderações extremamente profícuas de todos os presentes.

NOVAS TECNOLOGIAS E REGULAÇÃO: UMA ANÁLISE DO PL 872/2021 FACE AO DEVER DE DILIGÊNCIA DO ESTADO NA PROTEÇÃO DO DIRIETO À PRIVACIDADE

NEW TECHNOLOGIES AND REGULATION: AN ANALYSIS OF PL 872/2021 AGAINST THE STATE'S DUTY OF DILIGENCE IN PROTECTING THE RIGHT TO PRIVACY

Romulo Guilherme Leitao [1]
José Octávio de Castro Melo [2]
Rodrigo Pinheiro Sobreira Bedê [3]

Resumo

O presente artigo científico tem como objetivo analisar os modelos regulatórios sobre a inteligência artificial e a proteção ao direito fundamental de privacidade dos usuários das plataformas digitais em virtude da crescente demanda por dados pessoais e comportamentais. A investigação parte da análise dos diversos modelos de marcos regulatórios utilizados na União Europeia e nos Estados Unidos, ressaltando a sua maior ou menor efetividade na proteção ao direito de privacidade dos usuários das plataformas digitais. Neste contexto, a investigação parte da observação de lacuna regulatória no direito nacional e os desafios ético jurídicos na formatação de uma regulação global de proteção à privacidade de dados pessoais e comportamentais. O presente artigo busca identificar quais parâmetros ético-jurídicos devem ser adotados pelo marco regulatório da inteligência artificial no Brasil em consonância com as normas de direito internacional relativas ao tema. Para tanto, a pesquisa qualitativa concentrou-se na análise de dados bibliográficos, documentais, e na análise da legislação nacional e estrangeira. Por fim, chegou-se à conclusão de que é dever dos Estados promover a devida regulação da inteligência artificial como forma de prevenir lesão à direito fundamental à privacidade dos dados pessoais e comportamentais das plataformas digitais

Palavras-chave: Modelo regulatório, Inteligência artificial, Projeto de lei 872/2021, Dever de diligência do estado, Direito à privacidade

Abstract/Resumen/Résumé

This scientific article aims to analyze the regulatory models on artificial intelligence and the

---

[1] Pós-Doutor em Ciência Política Boston University, Massachusetts, EUA . Doutor e Mestre em Direito Constitucional pela Universidade de Fortaleza . Coordenador do Doutorado em Direito Constitucional - UNIFOR.

[2] Doutorando em Direito Constitucional -UNIFOR. Mestre em Direito -UFPE. Especialista em Direito Processual -UFSC. Professor Efetivo do Curso de Direito da Universidade Estadual do Piauí -UESPI

[3] Mestrando em Direito Constitucional - UNIFOR. Pós-graduação em responsabilidade civil e direito do consumidor - UNIFOR. Pós-graduando em direito digital e proteção de dados na Escola Brasileira de Direito

protection of the fundamental right of privacy of users of digital platforms due to the growing demand for personal and behavioral data. The investigation starts by analyzing the various regulatory framework models used in the European Union and the United States, highlighting their greater or lesser effectiveness in protecting the right to privacy of users of digital platforms. In this context, the investigation starts by observing the regulatory gap in national law and the ethical and legal challenges in formatting a global regulation for the protection of the privacy of personal and behavioral data. This article seeks to identify which ethical-legal parameters should be adopted by the regulatory framework of artificial intelligence in Brazil in line with the norms of international law on the subject. To this end, the qualitative research focused on the analysis of bibliographic and documental data, and on the analysis of national and foreign legislation. Finally, the conclusion was reached that it is the duty of states to promote the proper regulation of artificial intelligence to prevent injury to the fundamental right to privacy of personal and behavioral data on digital platforms.

Keywords/Palabras-claves/Mots-clés: Regulatory model, Artificial intelligence, Bill 872 /2021, State's duty of care, Right to privacy

1. INTRODUÇÃO

O progresso das novas tecnologias da informação propicia uma maior integração econômica e social entre as nações com o fluxo internacional de dados pessoais, sejam de origem pública ou privada, que demanda uma regulação protetiva cada vez maior dos direitos e liberdades fundamentais. A excessiva conexão com smartphones e a internet das coisas (IoT) produz uma infinitude de dados pessoais, que são a matéria prima da indústria da inteligência artificial, da qual extraem expressivo número de dados capturados através de algoritmos capazes de categorizar o consumidor e de prever quando ele está pronto para adquirir um certo tipo de bens.

A proteção do direito à privacidade dos dados pessoais, direito personalíssimo por excelência, exige que sejam tomadas por parte do Estado, medidas técnicas e organizacionais adequadas tanto quando da concepção do sistema de tratamento como da realização do próprio tratamento, a fim de manter a integridade desse direito fundamental.

Os recentes avanços oriundos da tecnologia da informação impulsionaram a conectividade da sociedade em rede propiciando ao usuário das plataformas digitais, acesso a bens e serviços ofertados, até então inimagináveis pela distância espacial que separava fornecedores, prestadores de serviço e consumidores por todo o planeta, contudo sem garantir efetiva da proteção da privacidade dos seus dados pessoais, expostos no ambiente do ciberespaço. Em razão disso, multiplicam-se os casos de utilização indevida de dados pessoais todos os usuários com violação ao direito fundamental à privacidade do usuário.

A tecnologia da informação avança a passos largos e revoluciona todas as áreas da vida humana. Inúmeros são os avanços na área da comunicação, em especial a conexão global através da internet e o constante fluxo de dados e informações instantâneas, a inteligência artificial, a robotização da indústria e dos meios de produção. Contudo, a mesma tecnologia que viabiliza o desenvolvimento também pode ser utilizada como instrumento de violação da privacidade psíquica e a identidade pessoal inclusive com práticas discriminatórias que ferem os direitos fundamentais.

Diante do contexto exposto indaga-se: quais parâmetros devem ser adotados pelo marco regulatório da inteligência artificial para garantir o direito à privacidade dos usuários nas plataformas digitais diante do crescente mercado de dados pessoais e comportamentais?

O presente artigo científico tem como objetivo analisar os impactos ao direito fundamental personalíssimo a privacidade de dados pelo uso de algoritmos que mapeiam comportamento nos usuários das plataformas digitais conectados pela tecnologia da internet das coisas (IoT).

Os objetivos específicos do presente artigo são: a) analisar os avanços e os riscos ao direito fundamental de proteção aos dados pessoais, advindo do uso do avanço da tecnologia da informação da maior conectividade propiciada pela internet das coisas (IoT); b) compreender o modelo capitalista de vigilância nas plataformas digitais na mineração de dados comportamentais do usuário; c) mapear os potenciais riscos de lesão ao direito à privacidade dos usuários nas plataformas digitais e d) analisar dever de diligência dos Estados na elaboração de políticas públicas e regulação do uso para as plataformas digitais como forma de proteção ao direito fundamental à privacidade dos dados pessoais diante das novas tecnologias de informação.

A relevância da pesquisa consiste na perspectiva da utilização de novas tecnologias como instrumentos capazes de mapear o comportamento humano através do uso de algoritmos em busca de lucro para as grandes empresas o que se pode denominar capitalismo de vigilância com potencial risco de lesão ao direito fundamental à privacidade dos usuários das plataformas digitais. A mesma tecnologia que abre as janelas do mundo ao usuário e o integra em uma comunidade global, é a mesma e o categoriza e discrimina.

Adota-se a pesquisa bibliográfica e documental. O referencial teórico é construído com base em pesquisas junto ao portal de periódicos científicos da Capes, por intermédio do acesso CAFE acessando a base de dados da *web of Science*, além de consulta aos periódicos especializados do portal Revista dos Tribunais e plataforma *Redalyc*. A busca foi realizada com a utilização das seguintes categorias: *Modelo Regulatório. Inteligência artificial. Projeto de Lei 872/2021. Dever de diligência do Estado. Direito à privacidade*.

As fontes documentais sobre a proteção ao direito fundamental à privacidade das plataformas digitais face ao mapeamento de seu comportamento através da mineração de dados pessoais a serviço de um modelo capitalista de vigilância foram pesquisadas nas bases de dados do IBGE e da ONU, no site *planalto.com*, na plataforma *V-Lex e* nos bancos de dados do Supremo Tribunal Federal (STF).

A abordagem da pesquisa tem base qualitativa com a análise da lacuna do Marco Legal de Inteligência Artificial para a proteção ao direito fundamental de proteção à

privacidade dos dados pessoais dos usuários e a não discriminação preditiva que ainda se encontra em fase de tramitação no Congresso Nacional.

2. A INTELIGÊNCIA ARTIFICIAL NOS DIAS ATUAIS

A inteligência artificial (IA) possui estudos que datam desde 1950 (TURING, 1950) e alcançou, após a chamada quarta revolução industrial, aspectos até então ignorados pela ordem jurídica constitucional, principalmente no que concerne sua capacidade em replicar e categorizar informações em velocidades incomparáveis à inteligência humana.

Há 25 anos atrás a *Deep Blue*, inteligência artificial criada pela Internacional *Business Machines* (IBM), foi capaz de vencer o campeão mundial de xadrez, Garry Kasparov (BBC NEWS, 2017). Em 2020, a Airbus, uma das principais empresas de fabricação de aviões no mundo, concluiu seus testes para informar que a utilização de aviões autônomos por meio de inteligência artificial, sem qualquer humano, já é realidade (BENQUET; DUVELLEROY, 2020).

Apesar da dificuldade de se trazer um conceito preciso e pacífico acerca do que seria a inteligência artificial (MACHADO, 2020), optou-se por escolher, para fins desta pesquisa, o conceito trazido Karl Manheim e Lyric Kaplan, segundo o qual a IA seria uma tecnologia que utiliza primordialmente *softwares* alimentados por algoritmos, para adaptar-se e emular a cognição humana, seja questionando, aprendendo ou agindo (MANHEIM; KAPLAN, 2019).

Em um mundo altamente globalizado onde tudo é conectado, esta tecnologia vem adquirindo formas extremamente realistas também nas mídias sociais, tornando-se cada vez mais difícil distinguir se um determinado usuário é ou não um algoritmo, acrescidos da dificuldade em saber como esses últimos funcionam, muitas vezes velados sob o manto do sigilo empresarial.

Algoritmos são como uma série de comandos direcionados a uma máquina, no intuito de resolver questões pré-estabelecidas. São comandos matemáticos presentes em grande parte do mundo digital, com objetivos e processos computacionais que transmutam determinados dados de entradas (*inputs*) em um objetivo final (*outputs*), geralmente se distanciando de qualquer parcialidade, apesar de não se manterem imune a interferências externas (SOUZA, 2018).

Se em 1997 a IBM conseguiu, com uma tecnologia de décadas atrás, que uma máquina vencesse o campeão mundial de xadrez, jogo conhecido pelas diversas

possibilidades de estratégia aplicáveis, o seria capaz da IA efetivar atualmente? A diferença, além da própria evolução esperada da tecnologia, se dá em face do montante de dados em circulação em 2022, muito maiores se comparados a 1997.

A precisão de algoritmos se baseia no montante de dados processados em suas interfaces, ou seja, quanto mais informações circulando na base de dados do sistema de IA, maiores as chances que o objetivo daquela programação seja mais efetivo. A própria rede do Facebook armazenou, em 2016, mais de 300 *peta bytes* a título de dados de usuários (JOLER; PETROVSKY, 2016).

Em face daquele cenário de grande montante de dados pessoais em circulação sem uma devida regulação e parâmetros para esta coleta, a União Europeia inovou ao criar o chamado Regulamento Geral sobre a Proteção de Dados (GDPR-GENERAL DATA PROTECTION REGULATION EU, 2016), documento apto a trazer uma proteção ao direito à privacidade não só a consumidores, mas a todos os titulares de dados pessoais. Inspirada na União Europeia, o Brasil também regulamentou este segmento, com a chegada da Lei Geral de Proteção de Dados (BRASIL, 2018).

Apesar da lacuna regulatória suprida com a chegada da LGPD, os sistemas de Inteligência Artificial ficaram fora do escopo da Lei, sendo mencionados brevemente em apenas um artigo desta, no tocante ao tratamento automatizado de dados pessoais. Não há qualquer menção, ainda que breve, sobre padrões éticos a serem seguidos no uso desta tecnologia, visto que sua utilização de forma irregular pode influir diretamente no direito à privacidade dos usuários das plataformas digitais.

Daí a necessidade de verificar se a regulação da inteligência artificial, nos moldes como fora elaborado a GDPR e LGPD em relação ao tratamento de dados pessoais, poderia maximizar a privacidade de usuários, com a adição de regras e padrões de compliance mínimos para os que atuam com esta tecnologia, apto a esclarecer este terreno ainda bastante nebuloso.

3. O DEVER DE DILIGÊNCIA DO ESTADO E A REGULAÇÃO DA INTELIGÊNCIA ARTIFICIAL

O Estado demonstra grande dificuldade para efetivação das políticas públicas pertinentes aos direitos fundamentais de conteúdo econômico, social e cultural. Neste sentido, uma política pública de proteção ao consumidor não se caracteriza como um ato isolado nem como a abstenção no que tange à prática de determinados atos, pois enquanto

os direitos individuais consistem em liberdades, os direitos sociais consistem em prestações (BREUS, 2007). Assim, uma das questões primordiais no que diz respeito à atuação do Poder Público refere-se à sua capacidade e velocidade de atualização e adaptação para aproveitar os recursos disponíveis com vistas a aprimorar a execução das políticas públicas (BUSCH, 2019).

A proteção da privacidade dos usuários conectados em rede também se sujeita a transparência em torno do desenvolvimento da inteligência artificial e dos algoritmos que mapeiam e classificam os consumidores de acordo com os seus interesses mercantis. Tanto os Estados quantas empresas privadas que se utilizam das novas tecnologias da informação e aqueles que fazem uso dos dados coletados devem manter transparência quanto ao tipo de sistema que usam e as finalidades que desejam atingir, ou mediante notificação de forma clara e objetiva, com especial atenção aos usuários que se encontram em situação de vulnerabilidade.

O Estado, portanto, deve fiscalizar e regular o uso de aplicativos de inteligência artificial que possam ter qualquer impacto na privacidade dos usuários com base em dados coletados, a fim de garantir uma transparência dos algoritmos. O Supremo Tribunal Federal reconheceu a proteção de dados pessoais como um direito fundamental em decisão que suspendeu a eficácia da MP 954/2020 e referendou a violação ao direito constitucional à intimidade, à vida privada e ao sigilo de dados, nas Ações Diretas de Inconstitucionalidade n°s. 6387, 6388, 6389, 6393, 6390, que obrigava as operadoras de telefonia a repassarem ao IBGE dados identificados de seus consumidores de telefonia móvel, tais como celular e endereço.

No mesmo sentido é o Projeto de Emenda Constitucional 17/2019[1] já aprovado pela Câmara dos Deputados e pelo Senado Federal, aguardando promulgação pelo Congresso Nacional, que tem como finalidade a inclusão do direito de proteção aos dados pessoais como garantias e direitos fundamentais consagrando a todo brasileiro, o direito de privacidade não somente na esfera física, mas também na esfera digital a proteção de seus dados pessoais nas relações de consumo em clara manifestação do Estado democrático de direito.

[1] A Proposta de Emenda Constitucional - PEC 17/2019, foi aprovada sob o número 115/2021 e reconheceu a constitucionalização da proteção de dados pessoais físicos e digitais como garantia e direito fundamental, no artigo 5º, da Constituição Federal, a qual ainda, fixa a competência da União para legislar sobre proteção e tratamento de dados pessoais, nos termos do artigo 22, da Carta Maior.

No cenário internacional a proteção de dados dos usuários nas plataformas digitais é tema da mais alta relevância no cenário econômico internacional, pois transcende as políticas públicas nacionais de proteção e segurança dos dados pessoais e não encontra mecanismo de segurança válidos para a proteção dos dados pessoais fora dos grandes blocos econômicos como a União Europeia.

Nesse cenário, teve bastante repercussão a decisão do *Caso Schrems II* pela Corte de Justiça da União Europeia em julho de 2020, que declarando como "inválida" a Decisão da Comissão Europeia (UE) 2016/1250 de 12 de julho de 2016 sobre a adequação da proteção fornecida pelo Escudo de Privacidade UE-EUA. Como resultado dessa decisão, o *Privacy Shield* [2] não é mais considerado um mecanismo válido para cumprir os requisitos de proteção de dados da UE ao transferir dados pessoais da União Europeia para os Estados Unidos.

O nível de segurança e proteção de dados esperada por um consumidor na Suécia é diferente do que se esperava razoavelmente em um país em desenvolvimento. A devida diligência na proteção de dados dos usuários da grande rede de conexão em massa é diretamente relacionada com a obrigação de prevenção, segundo a qual os Estados têm a obrigação de envidar os seus melhores esforços para prevenir danos a privacidade dos dados pessoais de acordo com o contexto local (MONEBHURRUN, 2022).

O Estado para cumprir o mandado constitucional deve atuar não só na esfera legislativa, editando leis para regular proteção dos dados dos usuários, mas também na esfera administrativa por meio da implementação de políticas públicas que promovam a aplicação imediata dos direitos já assegurados regramento nacional (BREUS, 2007).

No tocante às políticas públicas de defesa do consumidor, há previsão expressa no Código de Defesa do Consumidor (BRASIL, 1990) de dois importantes instrumentos: a Política Nacional das Relações de Consumo, que em linhas gerais, estabelece as diretrizes e cria instrumentos para a sua execução e do Sistema Nacional de Defesa do Consumidor, composto por órgãos federais, estaduais, distritais e municipais, além de entidades privadas de defesa do consumidor. Este Sistema era coordenado pelo Departamento

[2] *Privacy Shield* (escudo de proteção) e uma estrutura de proteção de privacidade projetadas pelo Departamento de Comércio dos EUA, pela Comissão Europeia e pela Administração Suíça, para fornecer às empresas em ambos os lados do Atlântico um mecanismo para cumprir os requisitos de proteção de dados durante a transferência dados pessoais da União Europeia e Suíça para os Estados Unidos em apoio ao comércio transatlântico. Disponível em https://www.privacyshield.gov/. Acesso em: 20 jun 2021.

Nacional de Defesa do Consumidor, que foi substituído pela Secretaria Nacional do Consumidor de Direito Econômico, no âmbito do Ministério da Justiça.

O dever de agir do Estado para proteção do consumidor é uma recomendação da Organização das Nações Unidas, em Assembleia Geral, que foi formalizada por meio da resolução nº 39/248, de 10 de abril de 1985. Nesta oportunidade, foi positivado o princípio da vulnerabilidade do consumidor, no plano internacional com diretrizes claras na construção de um modelo abrangente que envolve diversas áreas de atuação do Estado a fim de prover proteção ao consumidor.

Dentre elas destacam-se a promoção e proteção dos interesses econômicos dos consumidores, o acesso dos consumidores a uma informação adequada, a educação do consumidor e a possibilidade de compensação em caso de danos (FARIA, 2008). A construção legislativa de políticas públicas de proteção à privacidade dos dados pessoais deve desenvolver-se junto a todos os poderes do Estado e em conjunto com a sociedade disciplinando o direito de escolha por parte do titular dos dados, se quer ou não ter as suas informações divulgadas e compartilhadas (SCHREIBER, 2011).

As políticas públicas têm importante papel na defesa do direito de proteção de dados dos usuários e consumidores conectados em rede, digitalmente vulnerável no comércio eletrônico internacional face inúmeras situações cotidianas oportunizadas pelo avanço da tecnologia da informação agravada pelo isolamento social em tempos de pandemia. As políticas públicas implementadas pelo Estado são resultado de uma decisão política tomada sobre alternativas de políticas para atender uma determinada demanda e que apresenta uma característica central por ser revestida de autoridade soberana do Poder Público.

A proteção de dados pessoais do usuário é questão de abrangência multidisciplinar, orientando a natureza das Políticas Públicas e seus processos, na busca da construção de uma teoria geral, que tenha como objetivo, sintetizar teorias de diferentes ciências sociais, como as da ciência econômica (SOUZA, 2006). Tais políticas variam de acordo com o grau de diversificação da economia, como a natureza do regime social, como a visão que os governantes têm do papel do Estado e com o nível de atuação de diferentes grupos sociais, como partidos, sindicatos, associações de classe e outras formas de organização socia (BOBBIO, 1992), produto de um complexo e dinâmico processo de pressões políticas exercidas por grupos da sociedade civil e das predisposições políticas do governo em se deixar sensibilizar por estas pressões.

Nesse sentido, as políticas públicas podem ser compreendidas como instrumentos de execução de programas políticos baseados na intervenção estatal na sociedade com o escopo de garantir proteção à privacidade dos dados pessoais do usuário virtualmente conectado (APPIO, 2006) coordenando meios a para efetivar a proteção desse direito fundamental como "metas coletivas conscientes".[3]

A fixação das políticas públicas ocorre por meio dos mecanismos estatais de planejamento das ações, estratégias e metas para atingir a finalidade pública de forma eficiente, na prestação de ações e serviços públicos. A Constituição Federal é a base da fixação das políticas públicas, porque ao estabelecer princípios e programas normativos já fornece o caminho da atuação estatal no desenvolvimento das atividades públicas, as estradas a percorrer, obrigando o legislador infraconstitucional e o agente público ao seguimento do caminho previamente traçado ou direcionado (SANTIN, 2004).

A eficácia das políticas públicas de proteção aos dados pessoais é uma das principais questões da atualidade pois carece de atuação rápida e eficaz no intuito de garantir a segurança e a confiança na proteção desse direito fundamental sendo necessário que "[...] a tartaruga governamental seja capaz de se emparelhar com a lebre tecnológica e não seja soterrada pelos dados" (HARARI, 2016, p.327).

O progresso científico e tecnológico deve ser direcionado a beneficiar a humanidade e, portanto, deve ser obrigação dos Estados estabelecem medidas tendentes a atender a todos os usuários nas plataformas digitais garantindo-lhes sua vida privada e a intimidade, assim como a sua integridade psíquica mediante a criação de marcos regulatórios contra as eventuais ameaças da inteligência artificial.

No Brasil, o Projeto de Lei nº 21/20 que dispõe sobre o marco legal do desenvolvimento e o uso da inteligência artificial foi recentemente aprovado pela Câmara dos Deputados e segue tramitando junto ao Senado Federal, com grande expectativa de aprovação. O marco legal da inteligência artificial estabelece princípios, direitos e instrumentos de governança para a inteligência artificial e tem como principal fundamento o respeito aos direitos humanos e aos valores democráticos de igualdade, pluralidade, privacidade de dados e não discriminação. Os avanços oriundos da inteligência artificial deverão obedecer ao princípio da transparência relacionada ao seu uso e funcionamento (BRASIL, 2020).

[3] A expressão 'metas coletivas conscientes" foi utilizada por BUCCI, Maria Paula Dallari. Direito administrativo e políticas públicas. São Paulo: Saraiva, 2006.

O marco legal regulatório se faz necessário para impor limitações sobre acesso aos dados pessoais os usuários das plataformas digitais e o seu consequente uso, compartilhamento e negociação, combatendo a crescente e complexa opacidade do ambiente global do fluxo de dados públicos e privados trocados diariamente nas plataformas digitais, fortalecendo o direito à privacidade dados dos usuários.

Quanto mais avanço da tecnologia, maior risco de lesão ao direito privacidade dos usuários, e maior também a responsabilidade dos Estado em estabelecer medidas regulatórias e protetivas contra qual ação preditiva dos algoritmos utilizados pela tecnologia da inteligência artificial na mineração de dados pessoais comportamentais que possam ser utilizadas como produto negociável de categorização e discriminação da pessoa humana.

A Organização das Nações Unidas (ONU), por meio do Alto Comissariado dos Direitos Humanos, recomendou extremo cuidado no uso de aplicativos de inteligência artificial que não estejam de acordo com a legislação internacional de direitos humanos. Muito embora as novas tecnologias da informação possam trazer incalculáveis avanços na área científica, um grande desafio é garantir os padrões mínimos de privacidade estabelecidos pelos Marcos regulatórios nacionais e internacionais com especial atenção aos direitos humanos (ORGANIZAÇÕES DAS NAÇÕES UNIDAS, 2021).

Destaca-se sobretudo, os riscos negativos advindos da categorização dos usuários e de potenciais práticas discriminatórias nas plataformas digitais, demandando aos Estados um robusto sistema de controle e proteção à privacidade dos dados pessoais, impedindo que as novas tecnologias da informação e a hiper conectividade no capitalismo de vigilância possa ser utilizadas como instrumento de violação dos direitos humanos.

A regulação pressupõe a supervisão independente e imparcial de agências reguladoras que fiscalizem a inteligência artificial e o uso de algoritmos para mapear comportamento humano e categorizar os usuários em detrimento do direito fundamental à privacidade de dados pessoais. Os Estados devem garantir a devida diligência sobre os sistemas de inteligência artificial desenvolvidos pela big data, incentivando e exigindo das empresas a proteção ao direito da privacidade dos usuários das plataformas digitais.

Dessa forma os Estados podem identificar, prevenir e até mesmo mitigar os impactos nocivos das novas tecnologias sobre os direitos humanos em especial aos grupos que além da vulnerabilidade digital sofrem frequentemente discriminação tais como mulheres, negros, portadores de deficiência, idosos, lésbicas, gays, bissexuais, transgêneros, dentre outros. Cabem às agências reguladoras o monitoramento e a

avaliação de impacto das tecnologias da informação utilizadas como instrumento de vigilância do comportamento humano a fim de evitar práticas discriminatórias e utilização indevida de dados pessoais.

Os Estados devem direcionar seus marcos regulatórios para garantir que a inteligência artificial não seja utilizada de forma incompatível com os direitos humanos. Independentemente da responsabilidade das empresas que exploram o mercado de dados pessoais e das plataformas que mapeiam e comercializam tais dados. É dever do Estado agir proativamente mediante políticas públicas protetivas ao direito dos usuários e exigir condutas comerciais responsáveis a fim de mitigar os riscos de lesão ao direito à privacidade dos usuários, advindas da categorização dos usuários e de práticas discriminatórias tão comuns ao capitalismo de vigilância.

4. A LACUNA NORMATIVA E OS DESAFIOS DE PARÂMETROS GLOBAIS: ANÁLISE DO PL 872/2021

Na atualidade, o direito à privacidade sofre constante abalo pelo advento das novas tecnologias da informação e pela hiper conectividade dos usuários nas plataformas digitais. A utilização de algoritmos como instrumento preditivo o comportamento dos usuários consiste em forma invasiva de coleta e manipulação de dados pessoais frequentemente utilizados para categorizar pessoas de acordo com os interesses empresariais do capitalismo de vigilância (LYON, 1994).

O acesso do usuário às plataformas digitais é constantemente rastreado e mapeado pela inteligência artificial em constante processo de mineração de dados, cujas informações, muitas vezes são expostas em redes sociais ou em sites de prestação de serviços, que transformam os usuários em mercadorias (HAN, 2018) que podem ser precificáveis e comercializados pelos clientes reais daqueles que efetivamente controlam as plataformas digitais (SCHNEIER, 2015).

Uma vez na posse dos dados comportamentais do usuário que vão desde a ingênua navegação pelas redes sociais, pelos sites de buscas ou mesmo nas transações comerciais, as empresas são capazes avaliar e classificar os dados pessoais obtidos, frequentemente sem o conhecimento ou autorização do usuário, atribuindo-lhe valor monetário para posterior negociação no mercado virtual, ou até mesmo discriminando usuário que eventualmente tenha menor capacidade financeira (MENDES, 2014).

Se por um lado, o avanço da tecnologia da informação propicia inestimável avanço técnico que permite um melhor desenvolvimento de produtos e serviços, cada vez mais alinhados com a vontade do consumidor, assim como inestimável interação cultural no cyber espaço, por outro lado a inteligência utilizada para predizer o comportamento humano enquanto navega nas plataformas digitais no intuito de mapear as suas opções e preferências, transforma tais informações em um produto de fácil comercialização e de altíssimo valor para o novo modelo capitalista.

O Senado Federal também trouxe novas proposições regulamentadoras de sua autoria no tocante a IA, com o PL 872/2021, de iniciativa do Senador Veneziano Vital (MDB/PB). Este projeto, apesar de mais sucinto que o PL 21/20, possui uma padronização mais semelhante com a Lei Geral de Proteção de Dados (Lei nº 13.709/18) e aparentemente despertou maior interesse dos congressistas, com cerca de 18 emendas já propostas pelos senadores, com diversas diretrizes e fundamentos sobre o uso da IA, tanto no âmbito privado como no público.

Dentre uma das justificativas pela regulação da IA, tem-se que se faz necessário a consolidação de órgão reguladores com poder de exigir a devida adequação por parte daqueles que controlam o fluxo de dados. Através de mecanismos de fiscalização e controle rigorosos, procura-se conter o risco potencial de dano ao direito humano fundamental à privacidade de dados dos usuários, tendo em vista o constante e crescente desenvolvimento da inteligência artificial como instrumento eficaz de mapeamento do comportamento dos usuários no Ciberespaço.

Obviamente que, dentre as dezoito emendas propostas ao PL, não necessariamente haverá aprovação e inclusão de todas. Cumpre destacar, porém, algumas que chamaram a atenção e que podem fomentar ainda mais o debate sobre a regulação da IA no Brasil. A emenda nº 2 propôs incluir a proibição do uso da IA para a promoção e difusão de notícias falsas e mensagens preconceituosas. Afinal, um dos maiores entraves atuais no tocante a mercantilização e fomentação do uso de dados pessoais por tecnologias de inteligência artificial são sua possível utilização para a promoção e uso de notícias inverídicas (*fake news*), principalmente no âmbito das eleições.

Os direitos fundamentais possuem intima ligação com a ideia de dignidade da pessoa humana e com a limitação do poder do Estado (MARMELSTEIN, 2014) e nascem de reivindicações e lutas históricas estabelecidas na sociedade em busca de seu reconhecimento estatal e em documentos internacionais (COMPARATO, 2010) recebendo por parte do constituinte um tratamento especial quanto a sua aplicabilidade

imediata e refletindo uma ordem ao Estado que se incumbe permanentemente de sua concretização (SARLET , 2021).

A partir do século XIX, o direito de proteção à privacidade começou a figurar nos ordenamentos legais com forte ligação ao direito da personalidade humana e liberdade, atuando inicialmente como um meio de proteção da classe burguesa após as transformações da Revolução Industrial e com o surgimento da internet o direito à privacidade ganhou nova conotação abrangendo os dados pessoais, [4] fazendo surgir uma nova disciplina jurídica com regras sobre os mecanismos de processamento e legitimidade do controle de dados (RODOTÀ, 2008).

O ordenamento jurídico pátrio através da Lei Geral de Proteção de Dados, estruturou muito recentemente a proteção dos dados pessoais com forte influência nas diretivas europeias [5] e contextualizada com a disposições de direitos fundamentais previstas na Constituição da República, "cuja relação, propósito e alcance são fornecidos pela leitura da cláusula geral da personalidade" (DONEDA, 2019, p.259).

Em 25 de fevereiro de 2021 o pleno do Supremo Tribunal Federal STF julgou Ação Direta de Inconstitucionalidade nº 5962, em que figurou como requerente associação brasileira de concessionárias de serviço telefônico fixo como estado e outros ABRAFIX, a relatoria ficou a cargo do ministro Marco Aurélio Mendes de Farias Mello[6]. O Supremo Tribunal Federal julgou improcedente por maioria em sessão realizada por videoconferência em 25/02/2021 presidida pelo ministro Luiz Fux.

A associação referente pleiteava a declaração de inconstitucionalidade da lei do estado do Rio de Janeiro 4896 de novembro de 2006 que assegurava o direito de privacidade aos usuários de serviços de telefonia no que tange ao recebimento de ofertas de comercialização de produtos ou serviços por via telefónica ficando as empresas que prestam serviço de telefone fixo obrigadas a constituir a manter cadastro especial de

[4] Dados pessoais são todas as informações de caráter personalíssimo caracterizadas pela identificabilidade e pela determinabilidade do seu titular". in SARLET, Ingo Wolfgang. ***Os Direitos Fundamentais Sociais na Constituição de 1988***. Revista Diálogo Jurídico, Salvador, n. 1, v. 1, p. 1-46, abril/2001. Disponível em: http://www.direitopublico.com.br/pdf_seguro/revista-dialogo-juridico-01-2001-ingo-sarlet.pdf. Acesso em: 20 out 2022.

[5] Um exemplo de destaque é a Carta de Direitos Fundamentais da comunidade Europeia, na qual a proteção de dados é reconhecida como um direito fundamental autônomo. In RODOTÀ, Stefano. ***A vida na sociedade da vigilância*****:** a privacidade hoje. Rio de Janeiro: Renovar, 2008

[6] SUPREMO TRIBUNAL FEDERAL (STF). **ADI 5962**. Tribunal Pleno. Julgado em 25 de fevereiro de 2021. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5486862. Acesso em: 20 jun 2021.

assinantes que manifestem oposição ao recebimento via telefônico de ofertas de comercialização de produtos ou serviços.

Afinal, com um algoritmo de inteligência artificial objetivado primordialmente em influenciar eleitores para determinado candidato/espectro político por promoção de fake News, haveria um risco à democracia (FIGUEIREDO; FILHO, 2020). Acrescenta-se ao fato que muitos desses algoritmos de grandes corporações são pouco transparentes, no sentido de que não se sabe ao certo como os dados pessoais dos usuários são utilizados, quais seus critérios de análise e objetivos principais.

O próprio uso de contas automatizadas em períodos eleitorais é um problema atual, conforme pesquisa trazida pela Fundação Getúlio Vargas – FGV, onde concluíram que contas automatizadas motivaram cerca de 20% do debate público online no Twitter (FGV DAPP, 2017).

Dentre as emendas propostas temos a inclusão de incisos que protejam pessoas com deficiência e promovam a inclusão social; busca por conceito mais específico do que seria Inteligência Artificial; possibilidade de renúncias fiscais para aqueles que projetam seus negócios em IA etc. Outra emenda que merece destaque e que está em consonância com a União Europeia é a emenda nº 13, que propõe categorizar os riscos da IA a partir da forma que está sendo utilizada. Desta maneira, algumas atividades de IA se caracterizariam como risco inaceitável (usos efetivamente banidos), alto risco, risco limitado e risco mínimo.

Essa categorização está em compatibilidade com o plano da União Europeia de coordenação da Inteligência Artificial, que estabelece como um dos objetivos da comissão a elaboração de uma estrutura que priorize a segurança e o respeito aos direitos fundamentais em relação a IA categorizando está em diversos níveis de segurança, traçando como órgãos públicos e privados podem se adequar para que este uso seja realizado de forma regular (EUROPEAN COMMISSION, 2021).

O Brasil caminha, apesar dos curtos passos, em uma direção otimista no tocante à regulação da Inteligência Artificial. Apesar da lacuna regulatória existente, já existem projetos neste sentido e interesse dos órgãos legislativos no intuito de suprir o ordenamento jurídico com a regulação deste setor. O legislador brasileiro deve estar atento para que encontre um meio termo entre a proteção do direito à privacidade, de um lado, e a inovação tecnológica trazida por estas tecnologias, do outro.

Cumpre saber se, em um futuro não tão distante, o país poderá se situar globalmente como um país que trata o uso da IA com padrões globais mínimos aptos a garantir uma sociedade mais justa e segura.

5. CONCLUSÃO

A tecnologias da informação e a inteligência artificial exercem forte impacto no mundo moderno, aproximando a ficção da realidade e contribuindo de forma exponencial com os avanços científicos nos mais diversos setores do conhecimento humano. A tecnologia desenvolveu mecanismos integrativos entre homem e máquina com capacidade de acessar dados pessoais e comportamentais dos usuários, despertando profunda reflexão sobre os impactos éticos e jurídicos do uso dessas novas tecnologias para o acesso a dados dos usuários, bem como do potencial risco de utilização indevida que possa gerar considerável dano ao direito humano à privacidade dos dados pessoais todos os usuários ou prática discriminatória resultante do uso de algoritmos para a sua captação em benefício de um novo modelo capitalista mais invasivo e vigilante.

A internet das coisas (IoT) conecta pessoas e dados de forma muito rápida e eficiente, contribuindo para pesquisas na área de educação, saúde, transportes, contudo, o advento dessas novas tecnologias pode trazer danos imensuráveis aos direitos humanos em especial a privacidade dos seus dados pessoais e a garantia de sua utilização não discriminatória. Portanto se faz urgente e necessário, o preenchimento da lacuna legislativa de governança da inteligência artificial como instrumento de proteção a todos os direitos humanos.

As informações obtidas pela análise dos dados comportamentais dos usuários das plataformas digitais possuem inestimável valor económico, e representam ativo financeiro cobiçado pelo mercado internacional, que se valendo das novas tecnologias de captação, minera, analisa, categoriza o consumidor e direciona o mercado produtor com precisão preditiva, agregando mais valor às informações obtidas com ou sem o consentimento do usuário.

As políticas públicas de proteção ao direito fundamental à privacidade de dados pessoais e a regulação do uso da inteligência artificial para o mapeamento e categorização dos usuários conectados em rede, não acompanham o crescimento exponencial das novas tecnologias da informação, demandando especial atenção aos potenciais riscos aos direitos humanos e exigindo maior diligência por parte dos Estados.

A análise comportamental gerada pelos algoritmos fere a privacidade dos usuários que fazem uso da maior conectividade e interatividade que lhes é oferecida pela IoT e põe em risco a segurança direitos humanos com o vazamento constante de dados e potencial utilização discriminatória das informações neles contida. O modelo europeu e americano é utilizado por outros Estados, como referência para a criação de seus marcos regulatórios em busca de parâmetros éticos e jurídicos aliados com o princípio da precaução na proteção dos direitos humanos.

O uso das novas tecnologias deve ser regulado pelos Estados e perfeitamente alinhado com a garantia ao direito à privacidade, para que seu uso de forma adequada possa ser útil à sociedade cumprindo adequação e proporcionalidade sem prejuízo ético ou legal aos usuários. Da sua aplicação, não se espera qualquer lesão ou ameaça, seja por medidas invasivas de mapeamento do comportamento humano para fins meramente mercantis, o que possam gerar qualquer impacto discriminatório.

A necessidade de regulação e governança se faz necessário não apenas por interesses privados, mas também por interesses públicos, pois a tecnologia empregada nos algoritmos não distingue dados públicos e privados e representa uma ameaça à segurança internacional. Da mesma forma, parece ser imprescindível o compromisso de boas condutas por parte dos Estados e das empresas que atuam no ramo como mútua cooperação.

A responsabilização de entes públicos e privados controladores, gestores e beneficiários das informações coletadas deve ser capaz de garantir às vítimas de violação ao seu direito à privacidade o uso de medidas legais protetivas que lhe garantam a justa reparação. A transparência no uso das novas tecnologias da informação e o constante monitoramento do sistema de inteligência artificial são medidas preventivas que podem minimizar o risco de lesão ao direito humano.

REFERÊNCIAS

APPIO, Eduardo. **Controle judicial das políticas públicas no Brasil**. Curitiba, Juruá, 2006.

BBC NEWS. ***Deep Blue vs Kasparov***: How a computer beat best chess player in the world - BBC News. 2017. Disponível em: https://youtu.be/KF6sLCeBj0s. Acesso em 6 jun. 2022.

BENQUET, Lois; DUVELLEROY, Matthieu. ***Airbus concludes ATTOL with fully autonomous flight tests.*** AIRBUS. 2020. Disponível em:

https://www.airbus.com/newsroom/press-releases/en/2020/06/airbus-concludes-attol-with-fully-autonomous-flight-tests.html. Acesso em: 6 jun. 2022.

BOBBIO, Norberto. **A era dos direitos**. Rio de Janeiro: Campus, 1992.

BRASIL. Lei Geral de Proteção de Dados. **Presidência da República**. Brasília, 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 25 maio 2021.

BRASIL. Lei nº 21/2020. Projeto de Lei cria o Marco Civil da Inteligência Artificial e estabelece fundamentos, princípios e diretrizes para o desenvolvimento e aplicação da inteligência artificial no Brasil. **Câmara dos Deputados**. Disponível em https://www.camara.leg.br/propostas-legislativas/2236340. Acesso em: 20 jun 2022.

BRASIL. Lei nº 8.078 de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. **Presidência da República**. Disponível em http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 27 out 2022.

BRASIL. Projeto de Lei nº 872, de 12 de março de 2021. Dispõe sobre o uso da inteligência artificial. Brasília: **Senado Federal**, 2021. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/147434. Acesso em: 15 jun 2022.

BREUS, Thiago Lima. **Políticas públicas no Estado constitucional**: problemática da concretização dos direitos fundamentais pela Administração Pública brasileira contemporânea. Belo Horizonte: Fórum, 2007.

BUSCH, Christoph. ***Implementing Personalized Law***: Personalized Disclosures in Consumer Law and Data Privacy Law. University of Chicago Law Review. vol. 86, nº 2, 2019, p.309-332.

EUROPEAN COMMISSION. Coordinated Plan on Artificial Intelligence 2021 Review. 2021. Disponível em: https://digital-strategy.ec.europa.eu/en/library/coordinated-plan-artificial-intelligence-2021-review. Acesso em: 18 jun. 2022.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei geral de proteção de dados. 2. ed. São Paulo: Thomson Reuters, 2019.

FARIA, Heraldo Faria. **A proteção do Consumidor como Direito Fundamental em tempos de Globalização**. Revista Direitos Fundamentais e Cidadania, 2008.

FIGUEIREDO, Luiz Simão Leal de; FILHO, José Filomeno de Moraes. **Inteligência artificial e democracia**: os algoritmos podem influenciar uma campanha eleitoral? Revista Brasileira de Direitos Fundamentais & Justiça, v. 13, n. 41, p. 343-356, 2020. Disponível em: http://dfj.emnuvens.com.br/dfj/article/view/793. Acesso em: 24 ago 2020.

GENERAL DATA PROTECTION REGULATION EU. (GDPR). Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: 6 jun 2022.

HARARI, Yuval Noah**.** ***Homo Deus***: Uma breve história do amanhã. São Paulo: Companhia das Letras, 2016.

MANHEIM, Karl; KAPLAN, Lyric. ***Artificial Intelligence***: Risks to Privacy and Democracy. The Yale Journal of Law & Technology. New Haven, Connecticut. v.21. 2019. p.106-188. Disponível em: https://yjolt.org/sites/default/files/21_yale_j.l._tech._106_0.pdf. Acesso em: 6 jun. 2022.

MONEBHURRUN, Nitish. ***Diligentia quam in suis as a technique for a contextual application of the full protection and security standard: considering the level of development of host states in international investment law***. African Journal of International and Comparative Law. p. 596-611. Vol. 28, 2020.

ORGANIZAÇÕES DAS NAÇÕES UNIDAS. **ONU**. Disponível em: https://brasil.un.org/pt-br/144671-chefe-de-direitos-humanos-da-onu-pede-moratoria-para-inteligencia-artificial. Acesso em: 20 de jun de 2022.

ROBÔS, REDES SOCIAIS E POLÍTICA: Estudo da FGV/DAPP, aponta interferências ilegítimas no debate público na web. Levantamento mostra que contas automatizadas motivam até 20% de debates em apoio a políticos no Twitter, impondo riscos à democracia e ao processo eleitoral de 2018. Coordenador Marco Aurélio Ruediger. Rio de Janeiro: **FGV**, DAPP. 2017. Disponível em: http://dapp.fgv.br/robos-redes-sociais-e-politica-estudo-da-fgvdapp-aponta-interferencias-ilegitimas-no-debate-publico-na-web/. Acesso em: 18 jun. 2022.

SANTIN, Valter Foleto. **Controle judicial da segurança pública**: eficiência do serviço na prevenção e repressão ao crime. São Paulo: Revista dos Tribunais, 2004.

SCHREIBER, Anderson. **Direitos da Personalidade**. São Paulo: Atlas, 2011.

SEGUNDO, Hugo de Brito Machado. **Tributação e Inteligência Artificial**. Revista Jurídica Luso-Brasileira. Portugal. nº 1. Ano 6. 2020. p.57-77. Disponível em: https://www.cidp.pt/revistas/rjlb/2020/1/2020_01_0057_0077.pdf. Acesso em: 6 jun. 2022.

SOUZA, Celina. **Políticas Públicas: Uma revisão da literatura**. Sociologias, Porto Alegre, ano 8, n. 16, p.20-44. jul./dez. 2006.

SOUZA, Joyce (org.). **A sociedade de controle**. São Paulo: Hedra, 2018.

TURING. A.M. ***Computing Machine and Intelligence***. Mind. v. 59. p.433-460. 1950. Disponível em: https://www.csee.umbc.edu/courses/471/papers/turing.pdf. Acesso em: 6 jun. 2022.