REVISTA
ELETRÔNICA

DIREITO & TI

DIREITO & TI – PORTO ALEGRE / RS

WWW.DIREITOETI.COM.BR

VOL. 1

Nº 16 [MAIO/AGO]

ANO 2023

WB EDUCAÇÃO

ISSN 2447-1097

WB EDUCAÇÃO [CNPJ:41.653.466/0001-73]

Site: https://wbeduca.com.br/pt/

E-mail: revista@wbeducacional.com.br

REVISTA ELETRÔNICA DIREITO & TI [QUALIS CAPES B1]

Regras de submissão, cadastro e publicações: https://direitoeti.com.br/direitoeti

Editor-chefe: Emerson Wendt

Editora revisora: Valquiria P. C. Wendt

Dados Internacionais de Catalogação na Publicação (CIP)

Revista Direito e TI [recurso eletrônico] / WB Educação. - v. 1, n. 16 (maio/ago. 2023). Porto Alegre: WB Educacão, 2023.

Trimestral.
ISSN: 2447-1097.
Acesso em: <https://direitoeti.com.br/direitoeti>.

1. Direito - Periódicos. 2. Tecnologia da Informação - Periódicos. I. WB Educação.

CDD 340

Ficha catalográfica elaborada pela Bibliotecária Taís Amorim, CRB 10/2547

CONSELHO EDITORIAL

COMITÊ CIENTÍFICO

CRIMES CIBERNÉTICOS, CONVENÇÃO DE BUDAPESTE, *DATA* ATIVISMO + LIBERDADE DIGITAL, PROCESSO JUDICIAL + ACESSO À JUSTIÇA, TECNOLOGIA BLOCKCHAIN E RESPONSABILIDADE CIVIL: DESAFIOS EMERGENTES NA SOCIEDADE DE RISCO

Prezados leitores [e apreciadores da interseção entre o Direito e a Tecnologia da Informação],

Temos o prazer de apresentar a 16ª edição da Revista Eletrônica Direito & TI [mai/ago. 2023], um ponto de encontro dedicado a explorar a complexa relação entre vários temas emergentes.

Nesta edição, reunimos uma seleção eclética de artigos assinados por pesquisadores/as e especialistas em tecnologia/direito, todos convergindo para uma discussão central sobre o impacto das novas tecnologias no contexto jurídico e na sociedade em geral:

Artigo 1: Crimes Cibernéticos, falta de segurança e Legislação: um estudo de caso em Pernambuco, por *Gustavo Boudoux de Melo*.

Este artigo aborda a problemática dos crimes cibernéticos, a falta de segurança e as implicações legislativas, trazendo um estudo de caso específico e focado em Pernambuco. O autor, Gustavo Boudoux de Melo, analisa as diferentes facetas dos crimes cometidos no ciberespaço, destacando a importância da legislação na prevenção e repressão dessas práticas. Ao explorar a realidade em Pernambuco, o artigo busca fornecer *insights* sobre os desafios locais relacionados à segurança cibernética, destacando a necessidade de maior interação entre os órgãos públicos, empresas privadas e instituições de ensino.

Artigo 2: A adesão do Brasil à Convenção de Budapeste e o enfrentamento do cibercrime: entre a Cooperação Internacional e a expansão do Direito Penal, por *Isadora Donza Corrêa e João Araújo Monteiro Neto*.

Este artigo discute a adesão do Brasil à Convenção de Budapeste e seu papel no enfrentamento do cibercrime. Os autores, Isadora Donza Corrêa e João Araújo Monteiro Neto, exploram a dinâmica entre cooperação internacional e os benefícios da adesão à Convenção como forma de lidar efetivamente com as ameaças cibernéticas. A análise oferece uma visão aprofundada dos avanços legislativos necessários, inclusive nos processos de cooperação entre países.

Artigo 3: O *Data* ativismo em prol da proteção aos Direitos da Personalidade no Ciberespaço, por *Ana Elisa Silva Fernandes Vieira e Dirceu Pereira Siqueira*.

Ana Elisa Silva Fernandes Vieira e Dirceu Pereira Siqueira exploram o conceito de *data* ativismo (movimentos sociais por meio do ciberativismo) e seu papel na proteção dos direitos da personalidade no ciberespaço. O artigo destaca como a atuação proativa na defesa dos dados pessoais pode contribuir para a preservação da privacidade e autonomia dos indivíduos. A discussão oferece uma perspectiva crítica sobre o papel do ativismo digital na contemporaneidade.

Artigo 4: A utilização do Processo Judicial Eletrônico pelo Poder Judiciário e adoção de novas tecnologias como forma de democratização do Acesso à Justiça, por *Altair Resende de Alvarenga*.

Altair Resende de Alvarenga aborda a incorporação do Processo Judicial Eletrônico pelo Poder Judiciário e a adoção de novas tecnologias como um meio de democratizar o acesso à justiça, analisando, então, essa transição entre os meios analógicos e digitais de buscar a solução de conflitos na via judicial. O autor examina como a modernização dos procedimentos judiciais pode contribuir para uma maior eficiência e inclusão, proporcionando uma análise crítica sobre os desafios e benefícios dessa transição tecnológica.

Artigo 5: A Responsabilidade Civil aplicada a agentes autônomos de Inteligência Artificial no tratamento de Dados Pessoais Sensíveis, por *Rackel Farias Madeira e Anamaria Sousa Silva*.

Rackel Farias Madeira e Anamaria Sousa Silva exploram a responsabilidade civil relacionada aos agentes autônomos de Inteligência Artificial no tratamento de Dados Pessoais Sensíveis. O artigo analisa as questões éticas e legais associadas ao uso desses agentes, fornecendo uma reflexão sobre as alternativas e medidas necessárias para garantir a proteção dos dados pessoais em um cenário cada vez mais tecnológico.

Artigo 6: A nova tecnologia Blockchain: a revolução no mundo jurídico, por *Silvana Porciuncula de Moraes e Luciana Picanço de Oliveira*.

Silvana Porciuncula de Moraes e Luciana Picanço de Oliveira apresentam um estudo sobre a tecnologia B*lockchain* e sua revolução no mundo jurídico. O artigo explora as aplicações dessa tecnologia inovadora, destacando seu potencial para transformar os processos legais, prevenir fraudes, furto de dados e invasão de privacidade. A discussão abrange aspectos práticos e teóricos sobre esse "protocolo de confiança" caracterizado pela *Blockchain*, oferecendo uma visão abrangente sobre o impacto dela no Direito.

Artigo 7: A liberdade digital na Sociedade de Risco: perspectivas a partir da Proteção de Dados Pessoais, por *Pedro Henrique Hermes e Rogério Gesta Leal*.

Pedro Henrique Hermes e Rogério Gesta Leal investigam a liberdade digital na sociedade contemporânea, enfocando as perspectivas derivadas da proteção de dados pessoais. O artigo procura responder ao seguinte questionamento: "como o direito fundamental à liberdade no ambiente digital pode ser protegido pelo direito fundamental à proteção de dados pessoais e a Lei nº. 13.708/18 (Lei Geral de Proteção de Dados Pessoais)?", examinando a importância da proteção de dados pessoais como baliza na discussão entre sobre liberdade na Internet, especialmente a liberdade digital. A discussão propõe, então, reflexões críticas sobre a interseção entre liberdade, tecnologia e proteção de dados na era digital.

Embora os temas variem, todos os artigos-pesquisa desta edição compartilham o objetivo de abordar o impacto das tecnologias emergentes, a proteção de dados pessoais e as implicações legais/normativas na sociedade digital contemporânea. Esperamos que esta edição da Revista Eletrônica Direito & TI proporcione uma visão abrangente dessas questões interconectadas e promova discussões valiosas sobre o futuro do Direito e da Tecnologia da Informação.

Boa leitura!

Emerson Wendt,

Editor-Chefe,

Mestre e Doutor em Direito pela Universidade La Salle – Canoas,

Delegado de Polícia Civil PCRS, membro do Conselho Superior de Polícia Civil/PCRS.

SUMÁRIO

CRIMES CIBERNÉTICOS, FALTA DE SEGURANÇA E LEGISLAÇÃO: UM ESTUDO DE CASO EM PERNAMBUCO

CYBER CRIMES, LACK OF SECURITY AND LEGISLATION: A CASE STUDY IN THE STATE OF PERNAMBUCO

Gustavo Boudoux de Melo[1]

RESUMO: O presente artigo pretende trazer uma reflexão e discussão com relação aos crimes cibernéticos, pois com o avanço das tecnologias e internet, todos os dispositivos passaram a estar conectados, porém não há uma segurança quando se refere a proteção dos dados, há uma carência de legislações específicas, que venha a penalizar os criminosos, estes que acabaram se multiplicando principalmente após a pandemia e a chegada da COVID-19, onde se teve um maior isolamento e *lockdown*. O principal objetivo é analisar os crimes cibernéticos em Pernambuco, verificar quais são os crimes de maior incidência e quais são os maiores desafios para a segurança e defesa cibernética. A metodologia utilizada foi através das pesquisas bibliográficas, estudo de caso e pesquisa de campo junto a Delegacia de Crimes Cibernéticos de Pernambuco, com a utilização da abordagem investigativa, métodos quantitativos e aplicação de questionários. Como resultados encontrados, acredita-se que se houvesse uma maior interação entre os órgãos públicos, as empresas privadas e as instituições de ensino, bem como estudos e investimentos públicos e privados, e uma maior interdisciplinaridade entre a área do direito penal e as tecnologias de informação e comunicação, poderia se ter uma maior esperança de um dia poder ter uma certa segurança, cobertura jurídica e justiça, num país praticamente sem leis, anonimato e impunidade cibernética.

Palavras-chaves: crimes cibernéticos; direito digital; legislação; segurança cibernética.

ABSTRACT: This article intends to bring a reflection and discussion regarding cyber crimes, because with the advancement of technologies and the internet, all devices are now connected, but there is no security when it comes to data protection, there is a lack of legislation specific, which will penalize criminals, who ended up multiplying mainly after the pandemic and the arrival of COVID-19, where there was greater isolation and lockdown. The main objective is to analyze cyber crimes in Pernambuco, to verify which

[1] Doutorando em Direito na Universidade Católica de Pernambuco (PPGD - UNICAP). MBA Executivo em Segurança Cibernética pela Faculdade INTERVALE. Especialização em Crimes Cibernéticos pela Faculdade INTERVALE. Especialização em Direito Trabalhista pela Faculdade INTERVALE. E-mail: dir.gustavomelo@gmail.com. Currículo Lattes: http://lattes.cnpq.br/9393295457857318.

are the crimes with the highest incidence and which are the biggest challenges for security and cyber defense. The methodology used was through bibliographic research, case study and field research with the Pernambuco Cyber Crimes Police Station, using an investigative approach, quantitative methods and questionnaires. As results found, it is believed that if there were greater interaction between public agencies, private companies and educational institutions, as well as studies and public and private investments, and greater interdisciplinarity between the area of criminal law and technologies of information and communication, there could be greater hope of one day being able to have a certain security, legal coverage and justice, in a country practically without laws, anonymity and cybernetic impunity.

Keywords: cyber crimes; cybersecurity; digital law; legislation.

1 INTRODUÇÃO

Com a chegada e comercialização da internet no Brasil, em meados de 1994, as pessoas, computadores e equipamentos passaram a se comunicar e trocar informações, quebrando assim as barreiras e distâncias geográficas. Em torno de 2001, já se tinha internet nos telefones celular, aumentando assim a acessibilidade e mobilidade maior com a comunicação e informação.

De acordo com Wendt e Jorge (2013) da mesma forma que houve uma evolução dos recursos tecnológicos, também surgiram, cresceram e se aprimoraram as ameaças praticadas principalmente com o uso dos computadores. Já no final da década de 50 começaram a aparecer os códigos maliciosos, onde depois evoluíram para os vírus (1982), cavalos de Tróia (1986), evoluindo assim diversas outras ameaças. Só em 1988 foi que surgiu o primeiro antivírus para tentar combater e imunizar os computadores. E em 2004 foi quando surgiram os primeiros vírus para celulares, através da internet e *bluetooth*, abrindo espaço para a evolução e conectividade para os diversos tipos de dispositivos.

Acredita-se que atualmente a maioria da população brasileira deve ter pelo menos um telefone celular ou dispositivo conectado à internet, com acesso a vários aplicativos de troca de mensagens, informações, e-mails, bancos, compras de produtos e serviços, redes socais, dentre outros. Porém, como todo mundo tem acesso a mesma rede de internet, provedores, operadoras de telefonia, *wi-fi*, sites, aplicativos, dentre outros, onde

nesse mesmo espaço cibernético é compartilhado com todo tipo de pessoas e grupos, vai ter gente que "acobertados pela distância e pelo anonimato, tentam burlar a segurança dos equipamentos e dos sistemas informatizados de qualquer empresa, governo ou indivíduo e extrair benefícios indevidos da exploração desse bem chamado informação" (MANDARINO JUNIOR, 2011, p. 40).

Jesus e Milagre (2016, p. 16) consideram que todo o cidadão está vulnerável e sujeito a riscos neste espaço cibernético, pois "constitui-se presa fácil nas mãos de especialistas em crimes cibernéticos, os *crackers*[2], que exploram as intimidades dos sistemas e também dos processos desenvolvidos sobre a tecnologia da informação para a prática de delitos".

Por conta disso, se faz necessário se preocupar com a segurança da cibernética, e buscar proteger todas as informações e infraestruturas, que suportam as soluções de tecnologia da informação, composta pelos hardwares, softwares, servidores, roteadores, computadores, dispositivos, sistemas e serviços, de forma a montar uma "Estratégia de Segurança Cibernética para a Nação brasileira".

Para Mandarino Junior (2011, p. 45):

> Uma Estratégia de Segurança Cibernética para a Nação brasileira deve projetar e dimensionar os esforços necessários para proteger seus ativos de informação, suas infraestruturas críticas de informação, suas informações críticas; avaliar riscos; desenhar planos de contingências, para recuperação, ou não, de informações diante de desastres naturais; capacitar recursos humanos para responder, pronta e competentemente, a incidentes nas redes; garantir a privacidade das pessoas e das empresas presentes na sociedade da informação; e, como grande diferencial, ter a capacidade de aprender a desenvolver ferramentas de defesa. E ainda que essa Estratégia de Defesa Cibernética esteja apta a utilizar essas ferramentas e a própria informação como recurso ou arma, para assegurar a preservação do Estado brasileiro.

Partindo do princípio que o espaço cibernético é um local virtual "composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais

[2] Cracker é um vândalo virtual, alguém que usa seus conhecimentos para invadir sistemas, quebrar travas e senhas, roubar dados etc. Alguns tentam ganhar dinheiro vendendo as informações roubadas, outros buscam apenas fama ou divertimento (MORIMOTO, 2005).

transitam, são processadas e armazenadas" (DEFESANET, 2014), onde um dos recursos mais utilizados, e que facilita bastante é a comunicação, que pode ser realizada através de vídeo conferência, redes sociais, bem como com o uso da inteligência artificial, hipertextos, multimídia interativa, simulações, mundos virtuais (metaverso), dispositivos de tele presença, realidade aumentada, internet das coisas, dentre outras ferramentas, porém se faz necessário ter segurança nesses espaços que são compartilhados com o uso da internet, de forma que os dados e as informações das empresas, bem como os dados pessoais não venham a cair em mãos erradas, e causar algum tipo de dano ou prejuízo.

O presente artigo aborda o tema "crimes cibernéticos: a falta de segurança e legislação no Brasil", tem como objetivo analisar a questão dos crimes cibernéticos em Pernambuco, o que se tem feito para contribuir com a segurança no ciberespaço e o que se tem de legislação na área de direito penal e digital. Como objetivos específicos: Analisar quais são os crimes cibernéticos de maior incidência em Pernambuco; descrever o que se tem feito para minimizar a carência de legislação e insegurança cibernética; e verificar quais são os maiores desafios para a segurança e defesa cibernética.

A pesquisa em campo foi realizada junto com os servidores da Delegacia de Repressão aos Crimes Cibernéticos (DPCRICI) de Pernambuco.

Como problema de pesquisa, com base no crescimento das ocorrências e deligências relacionadas aos crimes cibernéticos, buscou-se verificar quais são os maiores desafios da DPCRICI-PE, bem como contribuir com sugestões para soluções e melhorias no combate ao crime cibernético de Pernambuco.

Procurou-se apresentar a rotina atual com relação aos crimes cibernéticos ocorridos junto a DPCRICI-PE, onde foi verificado quais são as principais carências e desafios relacionados aos crimes cibernéticos.

Para trazer embasamento teórico para este artigo e atender ao tema proposto em questão foram abordados alguns assuntos relacionados aos crimes cibernéticos e algumas leis específicas da área; direito penal e o Código Penal (CP); carência da legislação na área de direito digital no Brasil; e os desafios estratégicos para a segurança e defesa cibernética.

2 CRIMES CIBERNÉTICOS

Para um melhor entendimento com relação aos crimes cibernéticos, como definição são os "delitos praticados contra ou por intermédio de computadores (dispositivos informáticos, em geral)" (WENDT; JORGE, 2012, p. 18).

> Os crimes tecnológicos são aqueles que envolvem o uso de tecnologias computador, internet, caixas eletrônicos), sendo, em regra, crimes meios — ou seja, apenas a orma em que são praticados é que é inovadora. Têm como subespécie os crimes virtuais, informáticos ou cibernéticos (praticados pela internet), onde, apesar de se concretizarem em ambientes virtuais, os delitos trazem efeitos no mundo real (BARRETO; BRASIL, 2016, p. 36).

Várias condutas são consideradas crimes cibernéticos, como: acesso ilegítimo, interceptação ilegítima, interferência de dados ou dano informático, interferência em sistemas, uso abusivo de dispositivos, falsidade ou fraude informática, burla informática, furto de dados ou vazamento de informações, pichação informática, envio de mensagens não solicitadas e uso indevido informático.

Para Barreto e Brasil (2016, p. 37) os crimes cibernéticos podem ser classificados como (1) puros ou próprios; (2) impuros ou impróprios. A primeira classificação é caracterizada quando os "sistemas informatizados, bancos de dados, arquivos ou terminais são atacados pelos criminosos, normalmente após a identificação de vulnerabilidades, seja por meio de programas maliciosos ou, ainda, por engenharia social (golpista engana a vítima)". Seguem alguns exemplos de crimes cibernéticos (1) acordo com o Código Penal (BRASIL, 1940):

> Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita.
> Art. 163 - (Dano) Destruir, inutilizar ou deteriorar coisa alheia.
> Art. 266 - Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento.
> Art. 313-A. Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas

> informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano.
> Art. 313-B. Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente.

Os crimes cibernéticos classificados como impuros ou impróprios (2) "são aqueles onde o dispositivo tecnológico é utilizado como meio para a prática do delito, propiciando a sua execução ou o seu resultado (BARRETO; BRASIL, 2016, p. 39). São crimes comuns, que normalmente constam no Código Penal Brasileiro (BRASIL, 1940), onde o criminoso utiliza algum recurso tecnológico para cometer o delito, como nos exemplos a seguir:

> Art. 122 - Induzir ou instigar alguém a suicidar-se ou a praticar automutilação ou prestar-lhe auxílio material para que o faça.
> Art. 138 - Caluniar alguém, imputando-lhe falsamente fato definido como crime.
> Art. 139 - Difamar alguém, imputando-lhe fato ofensivo à sua reputação.
> Art. 140 - Injuriar alguém, ofendendo-lhe a dignidade ou o decoro.
> Art. 147 - Ameaçar alguém, por palavra, escrito ou gesto, ou qualquer outro meio simbólico, de causar-lhe mal injusto e grave.
> Art. 147-A - Perseguir alguém, reiteradamente e por qualquer meio, ameaçando-lhe a integridade física ou psicológica, restringindo-lhe a capacidade de locomoção ou, de qualquer forma, invadindo ou perturbando sua esfera de liberdade ou privacidade.
> Art. 153 - Divulgar alguém, sem justa causa, conteúdo de documento particular ou de correspondência confidencial, de que é destinatário ou detentor, e cuja divulgação possa produzir dano a outrem.

Esses artigos citados do CP (BRASIL, 1940) exemplificam apenas alguns crimes comuns da área de Direito Penal, porém existem muito mais, que quando são praticados com o uso de dispositivo tecnológico, principalmente com a utilização da internet e as redes sociais, os mesmos são tipificados como crimes cibernéticos, onde não maioria das vezes não se tem uma legislação específica. Importante se repensar sobre isso, pois a repercurssão, influência, manipulação, divulgação, propagação e disseminação pela internet é muito maior, causando danos e imapctos mais significativos do que se fosse por exemplo pessoalmente, como são os casos das *fake news*, *deepfakes*, *cyberbullying*, *stalking*, dentre outros.

Quando se trata especificamente das "condutas indevidas praticadas por computador" há uma classificação que "podem ser divididas em 'crimes cibernéticos' e 'ações prejudiciais atípicas'. A espécie 'crimes cibernéticos' subdivide-se em 'crimes cibernéticos abertos' e 'crimes exclusivamente cibernéticos'" (WENDT; JORGE, 2013, p. 18).

A seguir, apresenta-se as condutas indevidas praticadas por computador, ligadas aos crimes cibernéticos abertos, crimes exclusivamente cibernéticos e ações prejudiciais atípicas.

Figura 1 – condutas indevidas praticadas por computador

Fonte: Wendt e Jorge (2012, p. 20)

Os crimes cibernéticos abertos são aqueles praticados de forma tradicional ou por intermédio de computadores, que são usados para a prática do crime, porém também

podem ser cometidos sem o uso do computador. Alguns crimes determinados como abertos, como os crimes contra a honra; ameaça; importunação ofensiva ao pudor; falsificação de documentos; estelionato; furto mediante fraude; concorrência desleal; espionagem industrial; violação de segredo; apologia de crime ou criminoso; racismo; tráfico de drogas; atentado a serviço de utilidade pública.

Já nos casos dos crimes exclusivamente cibernéticos, próprios, aqueles cometidos com a utilização do computador ou outros equipamentos tecnológicos que tenha acesso à internet, percebe-se que há pelo menos um artigo de lei que especifique e tipifique determinado crime, trazendo assim as suas respectivas penas e sanções, com base em cada tipo e gravidade do crime em questão. Como são os casos de crime de pornografia infantil por meio de sistema de informática (art. 241-B, Lei nº 8.069/90); corrupção de menores em salas de bate papo da internet (art. 244-B, § 1 º, Lei nº 8.069/90) violar os direitos de autor de programa de computador (art. 12, Lei nº 9.609/98); inserção de dados falsos em sistema de informações (art. 313-A, Decreto-Lei nº 2.848/40); e crimes contra equipamentos da votação (art. 72, Lei nº 9.504/97).

No caso das ações prejudiciais atípicas, por ainda não serem consideradas como crime no Brasil, e não ter uma legislação específica, esse assunto será abordado no próximo tópico, trazendo uma reflexão com relação a carência de legislação na área de direito digital e penal, bem como as consequências de sua impunidade, além dos transtornos e prejuízos que podem ser gerados com cada tipo de ação atípica citada.

O presente estudo não tem a pretensão de aprofundar, esgotar e nem tão pouco detalhar todos os crimes cibernéticos, pois quando se trata dos artefatos, técnicas ou métodos, Jesus e Milagre (2016) citam 22 (vinte e duas) possibilidades para a prática de crimes informáticos; e 11 (onze) condutas informáticas que podem caracterizar um crime cibernético. Sendo assim, coloca-se como sugestão para uma pesquisa futura esse aprofundamento e detalhamento técnico com relação a todas essas possibilidades citadas, visando trazer apenas uma maior contribuição para a área jurídica.

Mesmo com todos esses tipos de crimes cibernéticos, além dos outros que ainda não são tipificados e caracterizados como delitos ou crimes, no que se refere a legislação

brasileira, direito digital e penal, ainda há uma carência muito grande com relação as leis e justiça no país, principalmente com relação as questões de investigação, monitoramento e rastreamento desses criminosos que vivem no anonimato, onde na maioria das vezes vivem e navegam pelo mundo mais obscuro, como por exemplo na *deep web* e *dark web*.

2.1 A carência de legislação na área de direito digital e penal no Brasil

Uma das formas de provar que ainda há muito o que se evoluir e atualizar junto a legislação penal brasileira, pois não tem uma previsão penal para as "ações prejudiciais atípicas", conforme apresentado na figura 1, ou seja, quando se trata desses tipos de ações e condutas ilícitas, o indivíduo não é punido porque ainda não há uma legislação específica, deixando assim o cidadão, que neste caso é a vítima, no prejuízo e transtornos, e o criminoso vai ficar impune.

> As "ações prejudiciais atípicas" são aquelas condutas, praticadas na/através da rede mundial de computadores, que causam algum transtorno e/ou prejuízo para a vítima, porém não existe uma previsão penal, ou seja: o indivíduo causa algum problema para a vítima, mas não pode ser punido, no âmbito criminal, em razão da inexistência de norma penal com essa finalidade (WENDT; JORGE, 2013, p. 18).

Para a legislação brasileira, conforme apresentado na figura 1, ainda não são considerados crimes, segundo Wendt e Jorge (2012, p. 20):

> - Acesso não autorizado a redes de computadores;
> - Inserção ou difusão de código malicioso;
> - Obtenção ou transferência não autorizada de dado ou informação;
> - Divulgação de informações pessoais.

Acredita-se que alguns fatores contribuem muito com essa carência da falta de legislação, como o surgimento tardio das novas áreas ou ramo do direito, como o direito digital, direito cibernético, crimes cibernéticos, direito penal informático e talvez mais algumas áreas afins.

Outro fator relevante também é a falta de comunicação e interdisciplinaridade entre duas grandes áreas, como a do direito e a tecnologia da informação e comunicação (TICs). Como também afirmam Jesus e Milagre (2016, p. 28) onde a "falta de apoio técnico – especialistas em tecnologia e segurança da informação, em setores legislativos – leva o legislador brasileiro à criação de tipos penais incoerentes".

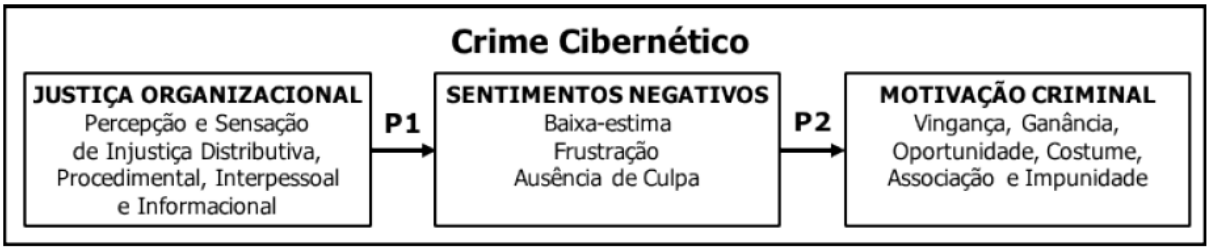
Como é de conhecimento comum, pode-se entender que se tratando de crimes cibernéticos no Brasil, o que vai servir como base de consulta legal é a Constituição Federal (BRASIL, 1988); Decreto-Lei nº 2.848, Código Penal (BRASIL, 1940); Decreto-Lei nº 3.689, Código de Processo Penal (BRASIL, 1941); Lei nº 12.735, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares (BRASIL, 2012a); Lei nº 12.737, dispõe sobre a tipificação criminal de delitos informáticos, conhecida como a Lei Carolina Dieckmann (BRASIL, 2012b); Lei nº 12.965, estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil, conhecido como o Marco Civil da Internet (BRASIL, 2014); Lei nº 13.772, para reconhecer que a violação da intimidade da mulher configura violência doméstica e familiar e para criminalizar o registro não autorizado de conteúdo com cena de nudez ou ato sexual ou libidinoso de caráter íntimo e privado (BRASIL, 2018); e por fim, Lei nº 14.155, para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet (BRASIL, 2021).

Uma outra situação que merece atenção, e que também há uma carência de legislação, percepção de impunidade e falta de monitoramento, e tudo isso também pode acabar incentivando as pessoas a cometerem crimes cibernéticos na própria empresa que trabalham, conforme pesquisa realizada por Garcia, Macadar, Luciano (2018), onde trazem como contribuição e acrescentam que as pessoas também podem ser motivadas a praticar crimes cibernéticos pelos sentimentos negativos de injustiça organizacional, além dos outros pontos comentados em questão.

Para Garcia, Macadar, Luciano (2018) a percepção e a sensação de injustiça organizacional provocam sentimentos negativos de baixa-estima, frustração e ausência

de culpa, despertando a vingança, ganância, oportunismo, costume, associação ou impunidade na empresa, que acabam sendo motivadas a cometerem crimes cibernéticos, principalmente por ter o conhecimento tecnológico e mais fácil acesso dentro da organização, conforme apresentado na figura 2.

Figura 2 – Modelo conceitual de crime cibernético por funcionários nas organizações



Fonte: Garcia, Macadar, Luciano (2018, p. 15)

Sendo assim, percebe-se uma necessidade de legislação específica de monitoramento e rastreamento das informações nas empresas, de forma que a mesma possa se proteger e salvaguardar de várias possibilidades negativas que podem ser ocasionadas por funcionários insatisfeitos, desmotivados, mal intencionados, problemáticos ou desonestos.

Visando contribuir para minimizar essa carência com relação a legislação brasileira no combate aos crimes cibernéticos, Jesus e Milagre (2016, p. 26) relatam um equívoco no que se refere a forma de condenação das técnicas informáticas, pois "estas são mutantes, nascem e morrem a qualquer momento, de acordo com a evolução dos sistemas, novas vulnerabilidades e plataformas tecnológicas", onde defendem que 'não se legisla sobre técnica' ou 'vulnerabilidade', pois o correto seria condenar as 'condutas praticadas por diversas técnicas', conforme proposta da teoria do TCC (Técnica, Comportamento e Crime), apresentada a seguir.

> Para que se possa conceber uma legislação minimamente eficiente, eficaz e que não precise ser complementada com o tempo, bem como para que se possa compreender o crime digital, importante se faz sistematizá-lo da seguinte forma:

> • **Técnica**: método, procedimento, *software* ou processo informático utilizado e que pode caracterizar um comportamento. Uma técnica pode ser executada manualmente ou por meio de subtécnicas, métodos automatizados ou ferramentas. A exemplo, um agente que obtém acesso a dados de um repositório pode estar utilizando a técnica de *sql injection*.
> • **Comportamento**: uma ação realizada por meio de uma ou mais técnicas, cometida por um ou mais agentes, por ação ou omissão, em face de redes de computadores, dispositivos informáticos ou sistemas informatizados. No mesmo exemplo citado acima, por meio da técnica *sql injection*, o agente praticou o comportamento "invasão de sistema informático".
> • **Crime**: um ou vários comportamentos, que utiliza uma ou mais técnicas, que ofende um ou mais bens ou objetos jurídicos protegidos pelo Direito. Mantendo o mesmo exemplo, a "invasão de sistema informático" pode ser ou não considerada crime, dependendo do país em que é praticada (JESUS; MILAGRE, 2016, p. 26).

Essa carência com relação a falta de legislação brasileira, principalmente no que se refere ao direito penal e digital, gera mais um desafio para a segurança e defesa cibernética.

2.2 Desafios estratégicos para a segurança e defesa cibernética

As empresas e instituições públicas e privadas precisam ter mais atenção com relação a questão da segurança, integridade dos dados e informações, principalmente no tocante a precisão e consistência dos dados, visto que há várias possibilidades e meios que podem comprometer a integridade dos mesmos, como o erro humano, podendo ser não intencional ou até mesmo malicioso; erros de transferência; bugs, vírus, *malware*, *hackers*, dentre outras ameaças; *hardware* comprometido; e compromisso físico para dispositivos.

Uma das alternativas para se proteger contra os crimes cibernéticos é fazer a contratação de *cyber* seguro, sistemas de monitoramento e rastreamento para os riscos cibernéticos, como também investimento em Inteligência Cibernética, Inteligência Artificial, *Machine Learning*, *backups* de segurança, espelhamento, *firewall*, criptografia, antivírus, assinatura digital, gestão de riscos de TI, dentre outros.

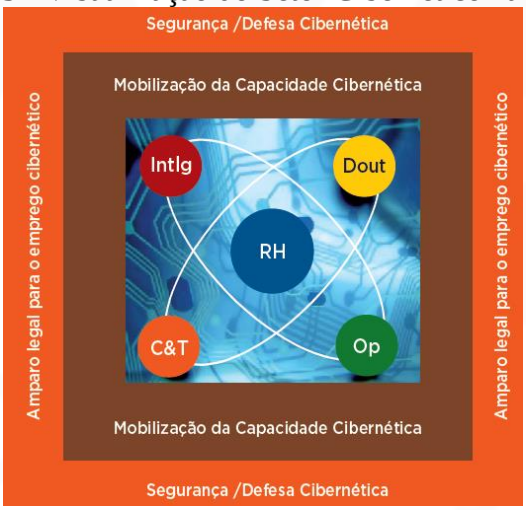
Segundo Barros, Gomes e Freitas (2011) a questão de capacitação dos recursos humanos deve ser uma atividade prioritária e indispensável, na qual a sua mobilização

deve ser integrada em quatro vetores, como: a inteligência; a doutrina; a ciência, tecnologia e inovação; e as operações.

Henriques (2021) afirma que um dos maiores desafios é com relação a capacitação de recursos humanos para a Defesa Cibernética, onde chama atenção de como deve ser trabalhada essa área, conforme apresentado a seguir.

> Para alcançar o objetivo de formar seus recursos humanos em cibernética o Exército precisou definir qual o universo a capacitar, bem como quais as capacidades necessárias para desempenhar as diversas atividades ligadas a Defesa Cibernética. Dentro desse contexto, definiu-se que o devemos entender que a capacitação em cibernética se desenvolve em 5 (cinco) níveis, quais sejam: USUÁRIO (Utiliza os sistemas de TI), TÉCNICO (Implementa sistemas de TI), ACADÊMICO (Programador, desenvolvedor de redes), PENTESTER (Aplica técnicas de defesa ativa), DESENVOLVEDOR 1 (Cria programas e técnicas de defesa), DESENVOLVEDOR 2 (Cria técnicas e programas contra sistemas operacionais) (HENRIQUES, 2021, p. 1).

Figura 3 - Visualização do Setor Cibernético na Defesa



Fonte: Barros, Gomes e Freitas (2011, p. 23)

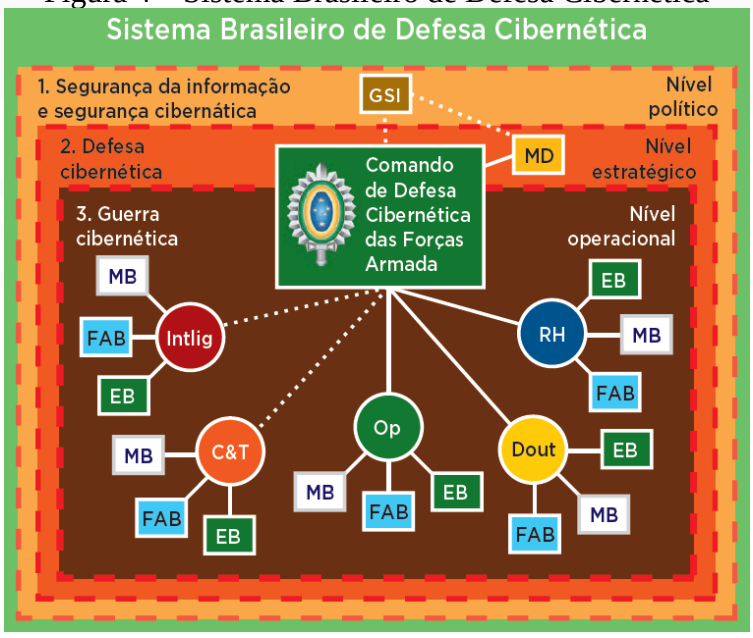
De acordo com Barros, Gomes e Freitas (2011) o Sistema Brasileiro de Defesa Cibernética deve ser implementado de forma integrada, como apresentas nas figuras 3 e 4.

Barros, Gomes e Freitas (2011, p. 27) destacam alguns desafios do setor cibernético no âmbito da defesa, como:

a. óbices de natureza cultural, associando as ações cibernéticas a atividades ilícitas de intrusão, quebra de privacidade das pessoas, roubo de dados etc.;
b. necessidade de conscientização de governantes e da sociedade como um todo em relação ao tema, decorrente do óbice anterior, que dificulta a obtenção da indispensável mobilização para a participação nas atividades de Segurança e Defesa Cibernéticas;
c. escassez de recursos financeiros ou não priorização do setor na alocação de recursos financeiros, também, em parte, decorrente dos óbices anteriores;
d. caráter sensível da atividade, dificultando a aquisição de conhecimento vindo do exterior; e
e. integração e atuação colaborativa incipientes dos diversos atores envolvidos.

Acredita-se que os principais desafios estratégicos seja manter o sistema brasileiro de defesa cibernética integrado e conectado, visto que o mesmo é composto por diversos órgãos, conforme apresentado na figura 4, que não haja uma rotatividade dos integrantes das equipes, que se desenvolvam e se qualifiquem continuamente na sua carreira e que se tenha recursos financeiros para os investimentos necessários como infraestrutura, equipamentos, tecnologias, sistemas e treinamentos específicos na área de segurança e defesa cibernética.

Figura 4 – Sistema Brasileiro de Defesa Cibernética



Fonte: Barros, Gomes e Freitas (2011, p. 26)

E por fim, Barros, Gomes e Freitas (2011, p. 28) destacam as ações estratégicas mais relevantes para que seja consolidado o Setor Cibernético na defesa, como:

> Assegurar o uso efetivo do espaço cibernético pelas Forças Armadas e impedir ou dificultar sua utilização contra interesses da defesa nacional;
> Capacitar e gerir talentos humanos para a condução das atividades do setor cibernético na defesa;
> Desenvolver e manter atualizada a doutrina de emprego do setor cibernético;
> Adequar as estruturas de CT&I das Forças Armadas e implementar atividades de pesquisa e desenvolvimento (P&D) para o setor cibernético;
> Cooperar com o esforço de mobilização militar e nacional para assegurar as capacidades operacional e dissuasória do setor cibernético.

Percebe-se que são muitos os desafios e que de fato se precisa ter estratégias para conseguir manter todo o sistema de segurança e defesa nacional funcionando, seguro e atualizado, além dos aspectos relacionados as doutrinas, legislações, ciência e tecnologia, pesquisa e desenvolvimento, e as relações internacionais, principalmente com o objetivo de troca de experiências, informações, expertises, dentre outros.

3 DESENVOLVIMENTO DA PESQUISA DE CAMPO

O objeto de estudo deste documento é formado pelos crimes cibernéticos e a falta de segurança e legislação no Brasil.

O objetivo foi analisar a questão dos crimes cibernéticos em Pernambuco, o que se tem feito para contribuir com a segurança no ciberespaço e o que se tem de legislação na área de direito penal e digital.

O universo e amostra da presente pesquisa foi com os servidores lotados na delegacia citada, onde contam atualmente com 8 (oito) servidores, porém um estava de férias e licença e o outro estava de licença médica, totalizando assim com 6 (seis) respondentes.

O desenvolvimento desta pesquisa teve um estudo bibliográfico, estudo de caso e pesquisa de campo junto a Delegacia de Crimes Cibernéticos (DPCRICI) de Pernambuco,

com a utilização da abordagem investigativa, métodos quantitativos, com aplicação de questionários com perguntas fechadas e objetivas, elaboradas de acordo com os assuntos e fundamentação teórica deste artigo em questão. Importante destacar que no estado de Pernambuco só tem apenas uma delegacia para atender os casos de crimes cibernéticos.

Para o desenvolvimento da pesquisa em campo foi aplicado um questionário fechado com 12 perguntas objetivas, visando analisar as ocorrências dos crimes cibernéticos na delegacia de repressão de Pernambuco, verificar quais são os seus maiores desafios, e quais são as sugestões para soluções e melhorias no combate ao crime cibernético.

4 ANÁLISES E RESULTADOS

Conforme questionário aplicado, o presente artigo teve as seguintes respostas.

1 - Com relação aos crimes cibernéticos abertos, qual desses tem o maior número de ocorrência na DPCRICI-PE? Os crimes mais comuns foram contra a honra, representando 66,7% e estelionato 33,3% das respostas.

2 - Com relação aos crimes exclusivamente cibernéticos, qual desses tem o maior número de ocorrência na DPCRICI-PE? Os que tiveram um maior número de ocorrências foram a pornografia infantil por meio de sistema de informática, com 66, 7%; e inserção de dados falsos em sistema de informações, com 33,3% das respostas.

3 – Com relação aos cibercrimes contra a pessoa, qual desses tem o maior número de ocorrência na DPCRICI-PE? As maiores ocorrências foram os crimes de difamação e injúria, ambos tiveram como 50% das respostas de cada.

4 - Com relação as condutas indevidas de ações prejudiciais atípicas, qual dessas tem o maior

número de ocorrência na DPCRICI-PE? O maior número de ocorrências com a inserção ou difusão de código malicioso, com 83,3%; e a obtenção ou transferência não autorizada de dados ou informação, com 16,7% das respostas.

5 - Na sua percepção, qual a principal motivação das pessoas que praticam um crime cibernético? A maior motivação para a prática dos crimes é a impunidade, com 83,34%; e a oportunidade, com 16,7% das respostas.

6 - Na sua percepção, qual das leis é a mais utilizada ou aplicada nesta Delegacia? As leis mais utilizadas são a Lei nº 12.965/2014 - Marco Civil da Internet, com 66,7%; e Lei nº 14.155/2021 - Violação de dispositivo informático, furto e estelionato, com 33,3% das respostas.

7 - Na sua percepção, qual o motivo que pode incentivar mais o cibercrime? Os motivos que mais podem incentivar os crimes são pela carência de legislação específica, com 50%; percepção de impunidade, com 33,3%; e falta de sistemas de rastreamentos, com 16,7% das respostas.

8 – Na sua percepção, o que mais contribui para essa carência de legislação específicas para o
cibercrime? O que mais contribui são a falta de qualificação e capacitação profissional, com 50%; falta de conhecimento do legislador, com 16,7%; e a falta de integração entre as forças de segurança pública, com 33,3% das respostas.

9 – A capacitação das pessoas em cibernética se desenvolve em cinco níveis, tais como: **Usuário** (Utiliza os sistemas de TI); **Técnico** (Implementa sistemas de TI); **Acadêmico** (Programador, desenvolvedor de redes); **Pentester** (Aplica técnicas de defesa ativa); e **Desenvolvedores** (Cria programas e técnicas de defesa ou programas contra sistemas operacionais). Qual capacitação em cibernética é a mais importante para o seu trabalho?

As capacitações mais importantes são no nível de desenvolvedores (Cria programas e técnicas de defesa ou programas contra sistemas operacionais) com 83,3%; e técnico (Implementa sistemas de TI), com 16,7% das respostas.

10 – Na sua percepção, qual o maior desafio do sistema brasileiro de defesa cibernética? Os maiores desafios são com a falta de investimento em segurança, com 83,3%; e falta de integração entre as forças de segurança pública, com 16,7% das respostas.

11 – Na sua percepção, o que mais poderia contribuir para uma maior segurança cibernética em Pernambuco? O mais poderia contribuir seria os investimentos em equipamentos e softwares, com 83,3%; e investimento em um sistema integrado de segurança cibernética, com 16,7% das respostas.

12 – Na sua percepção, o que poderia contribuir para agilizar o seu trabalho no combate ao cibercrime? O mais poderia contribuir para o combate ao cibercrime seria a integração entre as forças de segurança pública, representando 100% das respostas.

De acordo com as respostas apresentadas dos servidores da DPCRICI-PE, as maiores ocorrências em Pernambuco são os crimes contra a honra, estelionato, pornografia infantil por meio de sistema de informática, inserção de dados falsos em sistema de informações, difamação e injúria, inserção ou difusão de código malicioso, obtenção ou transferência não autorizada de dado ou informação.

A legislação mais utilizada foram a Lei nº 12.965/2014 - Marco Civil da Internet, e a Lei nº 14.155/2021 - Violação de dispositivo informático, furto e estelionato.

As principais motivações das pessoas e incentivos aos cibercrimes foram impunidade e a oportunidade; carência de legislação específica, percepção de impunidade, e a falta de sistemas de rastreamentos.

Ficaram evidentes as principais carências, como a falta de qualificação e capacitação profissional, a falta de integração entre as forças de segurança pública, e a falta de conhecimento do legislador.

E como principais desafios, que poderiam contribuir muito com o combate dos cibercrimes e trabalho da DPCRICI-PE, tiveram como maior destaque os pontos relacionados ao investimento na capacitação de desenvolvedores de soluções, programas e técnicas de defesa, investimento em segurança, equipamentos e softwares, bem como a integração entre as forças de segurança pública.

5 CONSIDERAÇÕES FINAIS

O tema escolhido é de extrema importância e urgência a ser debatido, bem como precisa de providências e soluções, principalmente pela possibilidade de trazer consequências negativas tanto para as pessoas e clientes, quanto para as empresas públicas e privadas, em função da vulnerabilidade, falta de segurança, monitoramento e rastreamento do espaço cibernético, principalmente das camadas que não tem nenhum tipo de regulação ou legislação, como na *deep web* e *dark web*, onde as pessoas navegam no anonimato.

De acordo com a Agência Senado (2021), a cada 11 segundos ocorre um ataque cibernético no mundo, e no último ano, provavelmente em razão da pandemia da covid-19, que levou mais pessoas a trabalhar em casa, houve um crescimento de 97% dos ataques cibernéticos, em relação a 2020.

Com base nas pesquisas e estudos, bem como em tudo o que foi apresentado nas análises e resultados, percebe-se que Pernambuco precisa investir e evoluir muito no combate aos crimes cibernéticos.

Acredita-se que se houvesse uma maior interação entre os órgãos públicos, as empresas privadas e as instituições de ensino, bem como estudos e investimentos públicos e privados, e uma maior interdisciplinaridade entre a área do direito penal e as áreas de sistemas e tecnologias de informação, poderia se ter uma maior esperança de um dia poder

ter uma certa segurança, cobertura jurídica e justiça, num país praticamente sem leis, anonimato e impunidade cibernética.

REFERÊNCIAS

AGENCIA SENADO**. Combate ao cibercrime é urgente, afirmam especialistas na CCT**. Publicado em: 15 dez. 2021. Disponível em: https://www12.senado.leg.br/noticias/materias/2021/12/15/combate-ao-cibercrime-e-urgente-afirmam-especialistas-na-cct. Acesso em: 31 maio 2022.

BARRETO, Alessandro Gonçalves; BRASIL, Beatriz Silveira. **Manual de investigação cibernética**: à luz do marco civil da internet. Imprenta: Rio de Janeiro, Brasport, 2016.

BARROS, Otávio Santana Rêgo; GOMES, Ulisses de Mesquita; FREITAS, Whitney Lacerda de (Orgs.). **Desafios estratégicos para segurança e defesa cibernética**. Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2011. Disponível em: http:/livroaberto.ibict.br/handle/1/612. Acesso em: 12 jan. 2022.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [2016]. Disponível em: http://www.planalto.gov.br/ ccivil_03/Constituicao/Constituicao.htm. Acesso em: 12 jan. 2022.

BRASIL. DECRETO-LEI Nº 2.848, DE 7 DE DEZEMBRO DE 1940. **Código Penal**. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 12 jan. 2022.

BRASIL. DECRETO-LEI Nº 3.689, DE 3 DE OUTUBRO DE 1941. **Código de Processo Penal**. Disponível em: http://www.planalto.gov.br/ccivil_03/decretolei/del3689.htm. Acesso em: 12 jan. 2022.

BRASIL. LEI Nº 8.069, DE 13 DE JULHO DE 1990. **Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências**. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 12 jan. 2022.

BRASIL. LEI Nº 9.504, DE 30 DE SETEMBRO DE 1997. **Estabelece normas para as eleições**. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9504.htm. Acesso em: 12 jan. 2022.

BRASIL. LEI Nº 9.609, DE 19 DE FEVEREIRO DE 1998. **Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências**. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9609.htm. Acesso em: 12 jan. 2022.

BRASIL. LEI Nº 12.735, DE 30 DE NOVEMBRO DE 2012. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, **para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências**. [2012a]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm. Acesso em: 12 jan. 2022.

BRASIL. LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012. **Dispõe sobre a tipificação criminal de delitos informáticos**; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. [2012b]. Disponível em: http://www.planalto.gov.br/ ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 12 jan. 2022.

BRASIL. LEI Nº 12.965, DE 23 DE ABRIL DE 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 12 jan. 2022.

BRASIL. LEI Nº 13.772, DE 19 DE DEZEMBRO DE 2018. Altera a Lei nº 11.340, de 7 de agosto de 2006 (Lei Maria da Penha), e o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), **para reconhecer que a violação da intimidade da mulher configura violência doméstica e familiar e para criminalizar o registro não autorizado de conteúdo com cena de nudez ou ato sexual ou libidinoso de caráter íntimo e privado**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13772.htm. Acesso em: 12 jan. 2022.

BRASIL. LEI Nº 14.155, DE 27 DE MAIO DE 2021. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), **para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet**; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm. Acesso em: 12 jan. 2022.

DEFESANET. Concepção Estratégica de Tecnologia da Informação. Portaria Nº 233, de 20 de Março de 2014. Aprova a Concepção Estratégica de Tecnologia da Informação. Disponível em http://www.defesanet.com.br/cyberwar/noticia/14799/EB---Concepcao-Estrategica-de-Tecnologia-da-Informacao/. Acesso em: 26 jan. 2022.

GARCIA, Plínio Silva de; MACADAR, Marie Anne; LUCIANO, Edimara Mezzomo. A influência da injustiça organizacional na motivação para a prática de crimes cibernéticos. **JISTEM - Journal of Information Systems and Technology Management [online]**. 2018, v. 15, e201815002. Disponível em: https://doi.org/10.4301/S1807-1775201815002. Acesso em: 24 jan. 2022.

HENRIQUES, Henrique de Queiroz. Os desafios da capacitação de recursos humanos para a Defesa Cibernética. **Observatório Militar da Praia Vermelha**. ECEME: Rio de Janeiro. 2021. Disponível em: http://ompv.eceme.eb.mil.br/defesa-cibernetica/guerra-cibernetica/392-des-c. Acesso em: 26 jan. 2022.

JESUS, Damásio de; MILAGRE, José Antônio. **Manual de crimes informáticos**. 1. Ed. São Paulo: Saraiva, 2016.

MANDARINO JUNIOR, Raphael. **Reflexões sobre Segurança e defesa Cibernética**. In. BARROS, Otávio Santana Rêgo; GOMES, Ulisses de Mesquita; FREITAS, Whitney Lacerda de (Orgs.). Desafios estratégicos para segurança e defesa cibernética. Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2011. Disponível em: http:/livroaberto.ibict.br/handle/1/612. Acesso em: 12 jan. 2022.

MORIMOTO, Carlos E. **Dicionário Técnico de Informática.** 3ª Ed., 2005. Disponível em: http://www.dominiopublico.gov.br/download/texto/hd000001.pdf. Acesso em: 24 jan. 2022.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos:** Ameaças e Procedimentos de Investigação. 1. ed. Rio de Janeiro: Brasport, 2012.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos:** Ameaças e Procedimentos de Investigação. 2. ed. Rio de Janeiro: Brasport, 2013.

A ADESÃO DO BRASIL À CONVENÇÃO DE BUDAPESTE E O ENFRENTAMENTO DO CIBERCRIME: ENTRE A COOPERAÇÃO INTERNACIONAL E A EXPANSÃO DO DIREITO PENAL

BRAZIL'S ACCESSION TO THE BUDAPEST CONVENTION AND CONFIGHTING CYBERCRIME: BETWEEN INTERNATIONAL COOPERATION AND THE EXPANSION OF CRIMINAL LAW

Isadora Donza Corrêa[1]

João Araújo Monteiro Neto[2]

RESUMO: O presente artigo científico tem como objetivo analisar a adesão do Brasil à Convenção de Budapeste, tratado internacional sobre Direito Processual Penal e Direito Penal, que foi desenvolvido como uma resposta à crescente ameaça de crimes cibernéticos, pretendendo à proteção da sociedade contra a criminalidade cometida no ambiente virtual. A Convenção de Budapeste foi promulgada no Brasil em 17 de abril de 2023 através do Decreto nº 11.419. Após fimar o tratado, o Brasil se comprometeu a adotar medidas para combater os crimes cibernético, penalizando infrações relacionadas

[1] Graduada em Direito pela Universidade de Fortaleza (2023). Estágio na Defensoria Pública do Estado do Ceará 2022.2 - 2023.1 Conhecimento Office: Excel (confecção de relatórios, gráficos etc.), Word (confecção de manuais, instrumentos contratuais, etc), e Power Point (criação de apresentações). Conhecimentos na Lei Geral de Proteção de Dados (LGPD). Colaboradora no Projeto: Ciências de Dados e Inteligência Artificial para Produtividade na Prestação Jurisdicional de 1 e 2 Grau - 2020 - atual. Colaboradora no projeto: Desenvolvimento Piloto de Soluções para a Automação Processual e Uso de Técnicas de Inteligência Artificial no Poder Judiciário. Aluna especial no mestrado em Informática Aplicada na Universidade de Fortaleza (Unifor). Noção básica em programação (Python). Currículo Lattes: http://lattes.cnpq.br/0547412133956929.

[2] PhD em Direito pela Universidade de Kent no Reino Unido. Curso de Aperfeiçoamento em Resposta a Incidentes pela Organização dos Estados Americanos em parceria com o Instituto de Ciberseguridade da Espanha (INCIBE) e a Universidade de Leon na Espanha. Ex pesquisador da Universidade de Malta e Voluntário no Mandato do Relator Especial da ONU para o Direito a Privacidade. Professor de Direito Digital, Proteção de Dados Pessoais e Engenharia Jurídica no curso de Direito da Universidade de Fortaleza. Advogado especializado em Proteção de Dados e Privacidade, Presidente da Comissão de Direito Digital da OAB/CE. Certified Information Privacy Professional/Europe (CIPP/E) pela International Association of Privacy Professionals (IAPP) e Privacy Fellow pela Onetrust. Coordenador do Grupo e Estudos de Estudos em Tecnologia, Informação e Sociedade - GETIS e com atividades nas áreas de Direito da Tecnologia da Informação, Governança e Regulação da Internet, Digital Human Rights, Privacidade e Proteção de Dados Pessoais, Inteligência Artificial e Cibersegurança.. Currículo Lattes: http://lattes.cnpq.br/4255484163600547.

a computadores e infrações cibernéticas. Para uma melhor compreensão do tema, buscou-se investigá-lo por meio de pesquisa bibliográfica, com o uso de referências teóricas em livros, artigos científicos, teses e monografias. Quanto à utilização dos resultados, a pesquisa é pura, por ter finalidade precípua a ampliação dos conhecimento sobre a temática. A pesquisa classifica-se como descritiva porque busca inicialmente registrar e analisar o tema sem manipulá-lo e explicativa pois aponta as causas que levam à sua adesão. Quanto à abordagem a pesquisa é qualitativa, enfatizando a compreensão e a interpretação do tema. No tocante aos fins, o presente artigo demonstra que a Convenção de Budapeste serve como importante referência para o Brasil no combate aos cibercrimes, incentivando avanços na legislação e na cooperação internacional no combate a essa modalidade criminosa.

Palavras-chave: Cibercrimes; Convenção de Budapeste; Mecanismos de cooperação internacional.

ABSTRACT: The objective of this scholarly article is to examine Brazil's compliance with the Budapest Convention, an international agreement on criminal procedure and criminal law. The convention was created in response to the increasing threat of cybercrimes, with the goal of safeguarding the public from illicit acts carried out in virtual spaces. On April 17, 2023, Brazil ratified the Budapest Convention with Decree No. 11,419. By joining the Budapest Convention, Brazil agreed to enact laws to combat cybercrimes and to make offenses involving computers and cybercrimes punishable by law. The topic was examined through bibliographic research, utilizing theoretical references from books, theses, scientific papers, and monographs in order to gain a deeper understanding of it. In terms of applying the findings, the study is strictly scholarly, with the primary goal being the advancement of knowledge in the field. The study is categorized as explanatory since it identifies the rationale behind the subject's adherence, and as descriptive since its primary goal is to document and examine the subject without altering it. The research employs a qualitative method, prioritizing the comprehension and interpretation of the topic. In terms of objectives, this article demonstrates how Brazil can tackle cybercrimes by using the Budapest Convention as a valuable guide, which promotes improvements in legislation and global collaboration in addressing this kind of illegal activity.

Keywords: international cooperation mechanisms; cybercrimes; Budapest Convention.

1 INTRODUÇÃO

No decorrer deste artigo científico, far-se-á uma análise da Convenção de Budapeste, tratado internacional sobre Direito Processual Penal e Direito Penal, que

objetiva a proteção da sociedade contra os cibercrimes, propondo a adoção de legislação adequada entre os países signatários em busca de uma cooperação internacional entre os membros. Criada em 2001, o tratado internacional foi originalmente estabelecido no Conselho da Europa, contando com mais de 60 países signatários.

O estudo busca esclarecer pontos críticos da adesão do Brasil à Convenção de Budapeste, tratado internacional, que serve de instrumento no combate aos crimes cometidos no ambiente virtual. Considerado um marco importante na cooperação internacional em investigações criminais de cibercrimes, o tratado, requer um esforço em conjunto no combate em escala global devido à dificuldade na identificação da autoria e materialidades nos crimes desta natureza.

O presente artigo tem como objetivos específicos responder a determinados questionamentos, tais quais: O que se entende pela Convenção de Budapeste e quais os crimes previstos no referido tratado internacional? O que são os cibercrimes e quais os mecanismos utilizados para combater esses crimes de tal natureza? E por fim, a promulgação da Convenção de Budapeste na legislação brasileira será vantajosa?

Tais questionamentos serão respondidos no decorrer do presente artigo, que será resumido em três tópicos. O primeiro tem como finalidade analisar o conceito de cibercrimes, com ênfase as classificações e divergências doutrinárias. Far-se-á posteriormente uma análise acerca do combate à cibercriminalidade, em que se mencionam os procedimentos de investigação no combate aos crimes cibernéticos e a problemática envolvida durante a investigação desses crimes.

O segundo tópico explora a Convenção de Budapeste, criada em 2001, na Hungria, pelo Conselho Europeu, que entrou em vigor no ano de 2004, objetivando impedir os atos praticados contra a confidencialidade, integridade e disponibilidade de sistemas informáticos de redes e dados. A terceira parte, trata da adesão do Brasil à Convenção de Budapeste, promulgada pelo Governo Federal, Decreto nº 11.419/2023, tratado internacional que incluirá novos tipos penais incriminadores com políticas no combate ao cibercrime.

Por fim, serão abordados os mecanismos de cooperação jurídica internacional incluídos pelo Decreto nº. 11.419/2023, no qual órgãos competentes dos estados atuam em conjunto em seus respectivos territórios, realizando atos pré-processuais ou processuais relevantes para a jurisdição estrangeira no âmbito da esfera penal.

2 CRIMES CIBERNÉTICOS

A era da tecnologia da informação teve seu início na segunda metade do século XX, quando ocorreram avanços tecnológicos significativos e uma maior disseminação de informações na sociedade. No século XXI, houve um crescimento da indústria dos computadores, com uma expansão cada vez maior do uso de recursos informáticos, como computadores, redes de fibras ópticas e tecnologia wireless etc. (COLLI, 2010, p. 15).

Dentre as principais novidades tecnológicas, encontra-se a internet. Criada na década de 90, é uma rede global de computadores que permite a transmissão de inúmeras informações com conteúdo diversos, podendo ser acessadas por computadores que ultrapassam as fronteiras geográficas e temporais de maneira imediata, facilitando a comunicação e o relacionamento entre as pessoas (COLLI, 2010, p.15).

Apesar de a tecnologia da informação ser um recurso valioso para a evolução da humanidade, cabe ressaltar que, alguns usuários desviam a sua finalidade para a preparação e consumação de infrações penais. Essa nova modalidade de delitos cometidos pelo ambiente virtual é comumente conhecida pela terminologia de crimes cibernéticos ou cibercrimes, que são crimes cometidos no ambiente computacional (VECCHIA, 2020, p. 52).

O Brasil é o segundo país com maiores prejuízos decorrentes de crimes cibernético. Conforme o Senado Federal, em apenas 3 meses do ano de 2019, o país registrou 15 bilhões de tentativas de ataques cibernéticos, com 59% dos ataques realizados com o fito de obter vantagens financeiras. (NICOLAI; ALVES, 2020).

2.1 Conceito

Os crimes cibernéticos, ou a criminalidade informática, podem ser conceituados como todo ato em que o computador ou meio de tecnologia de informação serve de meio para atingir um ato criminoso, ou ainda que, o objeto de um crime seja um computador ou um meio de tecnologia. (MARQUES; MARTINS, 2006)

Os crimes cibernéticos envolvem mais de um computador ou dispositivo telemático ou eletrônico, assim, devem estar conectados entre si por uma rede material ou imaterial. O instituto do cibercrime é a ligação entre a cibernética, o ciberespaço e os crimes informáticos, no qual esses meios de tecnologia são utilizados por usuários com o fito de cometer condutas delituosas. Portanto, para se ter um modelo de cibercrime, é necessário que o homem ao utilizar um computador, esteja por meio de uma rede de computadores, interligados no ciberespaço, cometendo condutas tipificadas como crimes (COLLI, 2010, p. 44).

Acerca da nomenclatura, os crimes cometidos na internet apresentam diversos termos doutrinários, qual seja: crimes informáticos, crimes digitais, crime informático-digital, *high technology* e *computer related crime*. Vale ressaltar que, esses crimes envolvem divergência quanto à definição, quanto à tipologia, e a classificação, no entanto, o termo cibercrime apresenta especial interesse, vez que a natureza deste é, em geral, de cunho transterritorial e transnacional. (SIMAS, 2014).

Conforme a Comissão Europeia, o cibercrime apresenta três tipos de atividades criminosas. A primeira delas abordam os crimes tradicionais, no qual são cometidos com o auxílio do computador juntamente com as redes informáticas. Em seguida, os crimes relacionados ao conteúdo, em que as publicações dos conteúdos ilícitos são realizadas através de meios de comunicação eletrônico. Por fim, estabelece os crimes exclusivos das redes eletrônicas, cometidos exclusivamente por meios informáticos (SIMAS, 2014).

Diante o exposto, pode-se concluir que a rede de internet apresenta uma grande fragilidade e meios para a perpetuação de cibercrimes, por ser uma rede de grande acesso ao público, bem como não ser regida por um ordenamento jurídico único que a discipline.

A existência de múltiplos ordenamentos jurídicos internacionais dificulta ainda mais a punição dos infratores, em razão da incompatibilidade procedimental e investigativa entre os diferentes países envolvidos em um cibercrime, sujeitando-se a sistemáticas processuais diversas (COLLI, 2010, p.45).

Por fim, pode-se concluir que, as infrações cometidas no espaço cibernético são chamadas de crimes informáticos ou crimes cibernéticos, que correspondem a qualquer ação ou omissão que possa ferir a política de segurança de uma instituição ou, ainda que possa atentar contra a segurança de um sistema informatizado.

2.2 Classificação dos cibercrimes

Na doutrina brasileira, não existe consenso sobre a expressão cibercrime, nem quanto à definição, nem quanto à tipologia e classificação destes crimes. Contudo, prevalece na doutrina a classificações dos cibercrimes entre crimes próprios e impróprios, de natureza formal, motivo pelo qual a consumação desses crimes acontece no momento da prática delitiva, independente do resultado naturalístico.

A primeira classificação aborda os crimes cibernéticos próprios ou exclusivamente cibernéticos, no qual são conceituados como toda atividade criminosa com principal objetivo a utilização de ambiente computacional, por isso, a execução do crime depende da utilização dos recursos tecnológicos como meio e objeto para a prática delituosa, sendo o ambiente computacional o objeto juridicamente tutelado (VECCHIA, 2020, p.53).

Além disso, nos crimes cibernéticos próprios, se referem ao uso da tecnologia da informação como meio necessário para a sua realização, assim, o autor do crime utiliza o sistema informático pertencente ao destinatário do crime, sendo o computador objeto e meio para a execução do crime. A título de exemplificação, pode-se mencionar o acesso não autorizado a sistemas informáticos, a interceptação de comunicações eletrônicas, fraudes eletrônicas, pornografia infantil etc. (VECCHIA, 2020, p.53).

Assim, é possível perceber que todos esses crimes utilizam a tecnologia da informação como meio para a sua realização, sendo importante destacar que essas práticas violam a privacidade, a segurança e a proteção dos dados pessoais das vítimas, gerando prejuízos e danos tanto para pessoas físicas quanto para empresas.

A segunda classificação aborda os crimes cibernéticos impróprios ou abertos, em que o ambiente computacional é o meio pelo qual é realizada a execução da conduta ilícita. Contudo, não necessariamente precisa do uso da tecnologia para se obter o resultado, ou seja, são crimes comuns que podem ser cometidos por meios diversos, como: divulgação de conteúdo ilícito na internet, comércio ilegal na internet, extorsão virtual, difamação online, entre outros (VECCHIA, 2020, p.53).

Ademais, todos esses crimes podem ser realizados sem a necessidade de se utilizar diretamente a tecnologia da informação como meio de ataque, mas, ainda assim, são considerados cibernéticos pelo fato de terem sido cometidos pelo uso de plataformas e sistemas-digitais. Os crimes cibernéticos impróprios utilizam a internet ou outras plataformas digitais como ferramentas para a prática de ilícitos, causando danos substanciais às vítimas.

2.3 Combate à cibercriminalidade

A investigação cibernética realizada no espaço cibernético ou em um dispositivo computacional é o campo de estudo da computação forense. Assim, a computação forense ou também chamada de perícia digital, tem como principal objetivo identificar, coletar, preservar e apresentar vestígios digitais com mais validade probatória em juízo. Os vestígios digitais são considerados informações que são deixadas em sistemas, dispositivos ou redes de computadores após a realização de atividades digitais, podendo ser exemplificado como: fragmentos de arquivos, textos, imagens, vídeos, registro de conexão à internet, bate-papo nas redes sociais, entre outros (NOGUEIRA, 2018).

A criminalística é a área responsável pela Forense Digital, no qual, aplica a ciência da computação e os procedimentos de investigação, no qual fornece evidências técnicas

para solucionar casos criminais, assim, esses métodos e técnicas realizados no objeto de perícia, auxilia na busca da materialidade e autoria dos incidentes de segurança e delitos perpetrados no ambiente cibernético (BRASIL, 2015).

Contudo, a investigação dos cibercrimes enfrenta uma problemática quanto as investigações preliminares desenvolvidas nesse ambiente, quanto à natureza do crime, os sujeitos, o tempo, o lugar de cometimento e as provas obtidas das infrações penais cometidas pela internet. Nesse contexto, devem-se analisar três elementos essenciais para a caracterização de um crime: a tipicidade, a ilicitude e a culpabilidade (BITENCOURT, 2006).

Segundo Bitencourt (2006), a tipicidade decorre do princípio da reserva legal, podendo ser brevemente definida como a conformidade entre o fato praticado pelo agente e a previsão do crime descrito no texto penal. Seguindo a mesma linha de pensamento do referido autor, a ilicitude seria a relação entre a conduta humana voluntária e o ordenamento jurídico, podendo assim ser definida como, um comportamento que contraria a ordem jurídica estabelecida em um território, em um determinado tempo.

A culpabilidade é o juízo que será feito sobre a reprovabilidade da conduta do agente, para deliberar sobre a prática ou não de uma infração penal. No Brasil, prevalece a teoria finalista, que apresenta três categorias na doutrina. A primeira delibera sobre a imputabilidade, em que trata de presunção de culpabilidade, podendo ser excluída pelos casos previstos em Lei. Em seguida, a segunda categoria trata sobre erro de proibição, em que o autor se equivoca acerca da ilicitude ou licitude do seu comportamento. Por fim, a terceira categoria trata sobre a exigibilidade de conduta diversa, sendo assim, é feito juízo de valor sobre o efeito das circunstâncias na conduta do autor (JUNQUEIRA, 2018).

Desta forma, para que ocorra a consumação de um crime cibernético, parte-se do pressuposto que, o fato deve ser típico, ilícito e culpável, e que seja lesivo a um bem jurídico tutelado pelo ordenamento jurídico brasileiro. Contudo, a tipicidade apresenta uma das principais problemáticas, devido ao surgimento diário de *malware* por programadores, *hackers* ou meros usuários, que se aproveitam das novas tecnologias para cometerem condutas danosas ou que ofereçam riscos a bens jurídicos cometidos através

da internet. Assim, ensejam situações que, apesar de serem ilícitas, são consideradas irrelevantes para o Direito Penal, por inexistir tipicidade caracterizadora da infração penal (COLLI, 2010, p.81).

A legislação brasileira, devido ao princípio da soberania, está limitada pela área territorial nacional para a punição dos crimes cibernéticos, o que dificulta as investigações policiais, já que a natureza destes delitos em sua maioria é de cunho transterritorial e transnacional. Neste seguimento, a existência de múltiplos ordenamentos jurídicos internacionais dificulta ainda mais a punição dos infratores, em razão da incompatibilidade procedimental investigativa entre os diferentes países envolvidos em um cibercrime, sendo assim, sujeitos e etapas diferentes estarão diante de sistemáticas processuais igualmente diversas (COLLI, 2010, p.81).

O principal meio para evolução das investigações policiais e a prevenção de cibercrimes deve ser por intermédio da cooperação internacional, necessitando que o Estado busque através de tratados e acordos internacionais sobre o tema, a obtenção da harmonização da legislação material e processual penal entre as nações.

Além disso, é necessário que os países signatários da comunidade internacional adequem a criação de unidades policiais especializadas em crimes informáticos, cibernéticos, e a conjugação de esforços entre autoridades investigadoras e provedores de internet (COLLI, 2010, p.82).

Na tentativa de uma colaboração internacional, o Conselho Europeu, no ano de 2001 firmou a Convenção de Budapeste, objetivando impedir os atos praticados contra a confidencialidade, integridade e disponibilidade de sistemas informáticos de redes e dados, assim, estabeleceu um extenso rol de diretrizes e regras para a adequação legal (material e processual) para a solução dos crimes cibernéticos nas relações internacionais (BRASIL, 2022).

Por fim, a cooperação internacional em matéria Penal e a internacionalização do Direito Cibernético irão garantir o enfrentamento do cibercrime, permitindo vínculo entre os sistemas judiciais internacionais, punindo e extraditando os responsáveis pela via da assistência jurídica mútua.

3 A CONVENÇÃO DE BUDAPESTE

O terceiro tópico abordará acerca da Convenção de Budapeste, enfatizando o processo histórico de criação, os seus principais elementos e os mecanismos de cooperação internacional implementados pelo tratado internacional.

3.1 Processo histórico da Convenção

Criada em 2001, a Convenção de Budapeste é um tratado internacional sobre direito processual penal e direito penal, no qual foi originalmente estabelecida no Conselho da Europa, englobando mais de 60 países signatários.

O Conselho Europeu criou o referido tratado objetivando realizar uma união mais estreita com os Estados-membros do presente tratado internacional, criando uma política criminal comum, que objetiva a proteção da sociedade contra os cibercrimes, adotando a legislação adequada entre os países signatários em busca de uma cooperação internacional entre os membros (BUDAPESTE, 2001).

A iniciativa para criação da convenção foi liderada pelo Conselho Europeu, com a participação de especialistas de países de todo o mundo e organizações internacionais. O processo envolveu diversas reuniões e audiências públicas para discutir o conteúdo e as questões legais em relação às implicações da criminalidade cibernética. A convenção foi desenvolvida como uma resposta à crescente ameaça de crimes cibernéticos que se tornaram cada vez mais sofisticados, difíceis de detectar e combatidos no âmbito nacional.

Além disso, o tratado internacional objetiva facilitar o intercâmbio de informações e a cooperação entre autoridades nacionais no combate à criminalidade cibernética, através da harmonização das leis nacionais e internacionais.

3.2 Delimitação dos crimes da Convenção de Budapeste

Assim como os crimes reais, os crimes virtuais têm sua jurisdição, a diferença é que os cibercrimes abordam inúmeras jurisdições devido as suas constantes modificações. As condutas criminosas cometidas na internet apresentam dificuldades na definição de tempo e lugar em que ocorreu a consumação do crime, por não haver fronteiras que estabeleçam o local no qual o criminoso realizou o delito. Desta forma, a complexidade de estabelecer o local da consumação do delito abre o questionamento pelo qual será a jurisdição competente para julgar o crime virtual cometido, e em qual país ficaria obrigado a responder pelo fato criminoso.

Diante da dificuldade apresentada em estabelecer a competência para julgar os crimes virtuais, a União Europeia, quando fica evidente que um crime ultrapassou as fronteiras do referido país, estabelece que a competência para julgar o fato criminoso será de todos os países envolvidos, assim, o combate para tal delito será solucionado através de acordos, no qual irão dispor a possibilidade de todos os países-membros de investigar o crime cometido fora de sua jurisdição.

A Convenção Europeia implementou medidas inéditas para o ambiente tecnológico, protegendo dados específicos de computadores, que caso fossem afetados, poderiam atingir diretamente direitos humanos e de liberdades individuais protegidos. Cabe ressaltar que, a Convenção Europeia faz referência expressa ao princípio da ofensividade, com o fito de indicar opções de criminalização de condutas que lesionem ou coloque em perigo um bem juridicamente tutelado que envolvem o abuso no uso de computadores.

Os países signatários da Convenção de Budapeste determinam sua jurisdição quando identificam a consequência real do crime praticado pela internet, assim, ao determinar o local do crime, será possível identificar a jurisdição competente para julgar a autoria do crime e a prova da materialidade. Cabe ressaltar que, alguns países vinculados a Convenção de Budapeste desenvolveram como solução de impasse a adoção da doutrina do efeito potencial do crime, permitindo a persecução penal, assim, caso o país signatário

encontre material hospedado em um servidor de outro país, e seja acessado em território nacional, os efeitos serão produzidos no território do acesso.

Neste seguimento, cabe salientar que existem três níveis de jurisdição na internet: o espaço físico, no qual, as pessoas são vinculadas ao espaço corpóreo que habitam, cabendo os cidadãos respeitar a legislação; os dos provedores de acesso, em que as pessoas se submetem as leis vigentes no país do referido provedor; por fim, os dos domínios e comunidades, que operam sem respeitar fronteiras internacionais ou de outros provedores.

A Convenção de Budapeste tem como objetivo a harmonia entre as legislações penais substantivas, estabelecendo o elemento dos delitos e outras previsões conexas sobre delitos de informática. Além disso, a referida convenção cumpre com o objetivo de alterar as legislações processuais nacionais, concedendo poderes de investigação e de persecução criminal, com o fito de combater delitos praticados com o uso de sistemas de computadores, ou outros delitos que envolvam provas obtidas mediante meios eletrônicos, com regime célere e efetivo de cooperação internacional.

No que consiste aos temas abordados na Convenção de Budapeste, a sua divisão está composta por quatro capítulos. O primeiro trata sobre os crimes contra a confidencialidade, integridade e disponibilidade de dados e sistemas de computadores, no qual está previsto o acesso ilegal à integralidade ou parte de sistema de computadores sem autorização, a interceptação ilegal, interferência ou danos em dados de computador, e por fim, a interferência em sistemas (BUDAPESTE, 2001).

O segundo capítulo da Convenção aborda os crimes já tipificados em legislações comuns, porém, os mesmos crimes sendo praticados por meio de computadores, como os crimes de falsificação eletrônica praticadas por meio de computadores e fraude informática. O terceiro capítulo preconiza as ofensas relacionadas à pornografia infantil. Por fim, no quarto capítulo, aborda os crimes relacionados à violação de direitos de autor em geral, ou condutas delituosas contra a propriedade intelectual (BUDAPESTE, 2001).

3.3 Principais elementos da Convenção de Budapeste

Inicialmente, a Convenção de Budapeste se inicia com a definição de conceitos e crimes cibernéticos até os mecanismos de cooperação entre os Estados-membros. Como dito anteriormente, a inclusão de alguns crimes inseridos pelo referido tratado podem ser estabelecidos como: acesso não autorizado a dispositivo eletrônico, interceptação ilegal a sistemas, interceptação ilegal de comunicações eletrônicas, pornografia infantil e fraude eletrônica.

Em seguida, a jurisdição estabelecida pela Convenção de Budapeste estabelece as bases da extraterritorialidade de lei em relação aos crimes cibernéticos, permitindo a cooperação entre os Estados-membros a operarem conjuntamente nas medidas legais contra os indivíduos ou organizações que cometeram tais delitos.

Cabe mencionar a cooperação internacional, mecanismo primordial da referida Convenção de Budapeste, em que prevê a cooperação entre os países membros na prevenção e investigação de crimes cibernéticos, incluindo a coleta e compartilhamento de informações e a extradição de suspeitos. Ademais, a proteção de dados pessoais também é considerado um elemento importante após a adesão do referido tratado internacional, em que a Convenção define as responsabilidades dos países a proteger os dados pessoais e de privacidade dos indivíduos, inserindo regras para o compartilhamento de informações e medidas de segurança.

Ademais, a proteção de dados pessoais também é considerado um elemento importante após a adesão do referido tratado internacional, em que a Convenção define as responsabilidades dos países a proteger os dados pessoais e de privacidade dos indivíduos, inserindo regras para o compartilhamento de informações e medidas de segurança. Por fim, insta destacar acerca do desenvolvimento de políticas públicas e estratégicas, em que a convenção necessita de políticas e estratégias nacionais para a prevenção e combate aos cibercrimes, devendo incluir medidas legais, técnicas, organizacionais e educacionais.

3.4 Mecanismos de cooperação internacional

A Convenção de Budapeste sobre Cibercrime estabelece vários mecanismos de cooperação internacional para combater a cibercriminalidade e prevenir violações dos direitos humanos no ambiente virtual. Além disso, a Convenção supramencionada também viabiliza a racionalidade do Direito Penal em cooperação internacional, tipificando condutas por meio da harmonização da legislação penal entre os países-membros, assim, garantindo o enfrentamento dos crimes cometidos pelo computador, por serem infrações que ultrapassam fronteiras internacionais, no qual haverá diálogo entre os diversos sistemas jurídicos internacionais (CASTRO, 2018).

O primeiro mecanismo de cooperação internacional estabelecido pela Convenção de Budapeste é o sistema de plantão 24 por 7, em que busca estabelecer e manter uma rede de contato com duração de 24 horas para permitir a rápida troca de informações sobre os crimes cibernéticos. A cooperação Internacional é outro mecanismo estabelecido pela Convenção de Budapeste, em que os Estados-membros devem cooperar entre si nas investigações em combate aos cibercrimes, incluindo o intercâmbio de informações relevantes e a implementação de ações conjuntas. O referido dispositivo está disposto no artigo 23, Capítulo III, Título 1, do Decreto nº 11.491/2023.

Dando seguimento aos mecanismos de cooperação, a extradição prevista pela Convenção de Budapeste prevista no artigo 24 do mesmo Decreto, estabelece regras para a extradição de indivíduos relacionados aos cibercrimes, desde que o tipo penal seja listado na legislação dos Estados-membros e seja possível a prova da materialidade do delito e a autoria.

Diante o exposto, devido os mecanismos de cooperação internacional impostos pela Convenção de Budapeste, pode-se concluir que visa promover a prevenção dos crimes cometidos no ambiente virtual, bem como a proteção dos direitos humanos no ambiente digital.

Ressalta-se ainda que, esses dispositivos são importantes para garantir que as autoridades policiais de diferentes países possam colaborar efetivamente em

investigações de crimes digitais, evitando lacunas no combate à cibercriminalidade decorrentes das fronteiras geográficas.

4 O PROCESSO DE ADESÃO DO BRASIL À CONVENÇÃO DE BUDAPESTE

O processo de adesão do Brasil à Convenção de Budapeste sobre Crimes Cibernéticos começou em 2009, com a assinatura do documento em uma cerimônia realizada em Estrasburgo, na França. Na época, o Brasil foi representado pelo então ministro de Relações Exteriores, Celso Amorim.

Após a assinatura, o Brasil iniciou o processo interno necessário para tornar a convenção parte de sua legislação nacional. Em 2011, foi elaborado um relatório detalhado sobre a adesão, que passou por avaliação de diversas áreas do governo, incluindo as áreas de Justiça, Segurança Pública e Relações Exteriores (BRASIL, 2019).

Ao aderir à convenção, o Brasil se comprometeu a desenvolver e fortalecer seus mecanismos jurídicos, administrativos e técnicos para combater os crimes cibernéticos. Isso inclui o desenvolvimento de leis e políticas nacionais para prevenir e investigar esses crimes, promover a cooperação internacional na área de crimes cibernéticos e reunir evidências para processar aqueles que cometem crimes online.

Datada em 15 de dezembro de 2021, a Convenção de Budapeste foi aprovada pelo Senado e promulgada pelo Governo Federal em 17 de abril de 2023, em Brasília, Decreto nº 11.419, que traz a decisão publicada no Diário Oficial da União (DOU), no dia 12 de abril de 2023.

4.1 Adequação dos mecanismos de criminalização

Inicialmente, cabe ressaltar que a legislação penal brasileira já previa alguns crimes estabelecidos pela Convenção de Budapeste, tais como o acesso não autorizado a dispositivos eletrônicos, interceptação e divulgação não autorizada de informações pessoais, pornografia infantil e fraudes informática. Contudo, a legislação brasileira

precisou adaptar-se para atender a diversos requisitos da convenção, como a implementação da nova definição de crimes cibernéticos e as novas tipificações de delitos listados que devem ser criminalizados pelos Estados-membros.

Dando início ao comparativo entre a Convenção de Budapeste e a lei brasileira, se dará início pela Seção 1, Título 1, artigo 2º, do Decreto nº 11.491/2023, em que se trata do acesso ilegal a um sistema de informação, no qual o acesso doloso a um sistema protegido por senha objetivando obter dados de computador ou outro meio fraudulento é considerado crime, conforme a seguinte redação:

> [...] Cada Parte adotará medidas legislativas e outras providências necessárias para tipificar como crime, em sua legislação interna, o acesso doloso e não autorizado à totalidade de um sistema de computador ou a parte dele. Qualquer Parte pode exigir para a tipificação do crime o seu cometimento mediante a violação de medidas de segurança; com o fim de obter dados de computador ou com outro objetivo fraudulento; ou contra um sistema de computador que esteja conectado a outro sistema de computador. (BRASIL, 2023).

Cabe ressaltar que, a legislação brasileira já protegia o acesso ilegal, sendo regulado pela Lei Carolina Dieckmann, em seu artigo 154-A, Lei nº 12.737 de 2012, que ficou conhecida como a Lei dos Crimes Eletrônicos, no qual prevê como conduta ilegal a obtenção não autorizada de dados armazenados em dispositivos eletrônicos, como celulares e computadores, configura o crime de "acesso não autorizado" e é punível com pena de três meses a um ano de detenção, além de multa. O mesmo tipo de punição é aplicável a quem produz, distribui ou comercializa programas de computador voltados para a prática deste crime. Segue redação do dispositivo legal supramencionado:

> Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita. (BRASIL, 2012).

Além disso, a legislação brasileira estipula punição para o acesso não autorizado a um sistema informático ou de telecomunicações. Isso inclui, por exemplo, a obtenção de informações de uma rede ou sistema sem autorização ou permissão expressa do

proprietário ou administrador do sistema. Essa lei é aplicável a qualquer pessoa que obtenha esses dados sem autorização, independentemente do motivo ou finalidade do ato. Essa lei se aplica também a quem pratica essa atividade com o objetivo de obter vantagem econômica ou financeira.

Assim, pode-se concluir que, a legislação brasileira já dispõe de medidas para prevenir, investigar e punir o acesso não autorizado a dispositivos eletrônicos, o que vai ao encontro dos padrões estabelecidos pela Convenção de Budapeste. Contudo, é importante observar que a legislação precisa ser constantemente atualizada e aprimorada para acompanhar as constantes mudanças na tecnologia e nas ameaças dos crimes cibernéticos.

Dando seguimento a análise da legislação brasileira anterior com a nova lei da Convenção de Budapeste, o artigo 3º, Seção 1 do Decreto nº 11.491/2023 aborda a tipificação de interceptação ilícita, em que aborda condutas ilícitas aos indivíduos que interceptam comunicações eletrônicas, com objetivo fraudulento ou praticado contra um sistema de computador que esteja conectado a outro sistema de computador. A título de exemplo, pode-se mencionar o indivíduo que intercepta comunicações eletrônicas, como e-mails ou mensagens criptografadas. Segue a redação do artigo mencionado acima:

> [...] Cada Parte adotará medidas legislativas e outras providências necessárias para tipificar como crime em sua legislação interna a interceptação ilegal e intencional, realizada por meios técnicos, de transmissões não-públicas de dados de computador para um sistema informatizado, a partir dele ou dentro dele, inclusive das emissões eletromagnéticas oriundas de um sistema informatizado que contenham esses dados de computador. Qualquer Parte pode exigir para a tipificação do crime o seu cometimento com objetivo fraudulento ou que seja praticado contra um sistema de computador que esteja conectado a outro sistema de computador. (BRASIL, 2023).

Apesar de a tipificação supramencionada ser incluída pela promulgação da Convenção de Budapeste em 2023, a legislação brasileira tipifica esse delito na Constituição Federal em seu artigo 5º, inciso XII, estabelecendo que é inviolável o sigilo das comunicações telegráficas, de dados e telefônicas, exceto por ordem judicial, para

fins de investigação criminal ou instrução processual penal. Assim segue a redação do dispositivo mencionado acima:

> Art. 5º [...]: XII - e inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal. (BRASIL, 1998).

Além disso, a autorização da interceptação telefônica ou telemática é regulada pela Lei 9.296/96, que estabelece os critérios e procedimentos a serem seguidos pelas autoridades encarregadas da aplicação da lei. Assim, para configurar o crime de interceptação ilícita no Brasil, a legislação penal exige que a interceptação tenha ocorrido sem autorização judicial ou em desacordo com as disposições legais. A pena prevista para esse delito é de reclusão, de dois a quatro anos, e multa.

É importante destacar que, no Brasil, a interceptação telefônica ou telemática só pode ser realizada por autorização judicial especificamente solicitada para este fim, com fundamentação adequada e em cumprimento com todos os critérios estabelecidos pela lei. Além disso, a autorização de interceptação deve ter fim específico, não podendo ser utilizada ou mantida após o término do objetivo determinado pela autoridade judicial.

Dessa forma, a legislação brasileira já prevê medidas para prevenir e reprimir a interceptação ilícita de informações eletrônicas, atendendo aos requisitos da Convenção de Budapeste. É importante ressaltar que a proteção da privacidade dos usuários da internet e a manutenção de um ambiente eletrônico seguro são fundamentais para a garantia dos direitos humanos e do Estado Democrático de Direito.

Dando continuação ao Decreto nº 11.491/2023, insta salientar em seu título 2, o artigo 7º, no qual aborda sobre o tema de falsificação informática, consistindo em um ato em que o indivíduo distribui ou utiliza um *malware*, objetivando danificar ou obter informações de um sistema.

> [...] Cada Parte adotará medidas legislativas e outras providências necessárias para tipificar como crimes, em sua legislação interna, a inserção, alteração, apagamento ou supressão, dolosos e não autorizados, de dados de computador,

> de que resultem dados inautênticos, com o fim de que sejam tidos como legais, ou tenham esse efeito, como se autênticos fossem, independentemente de os dados serem ou não diretamente legíveis e inteligíveis. Qualquer Parte pode exigir, para a tipificação do crime, o seu cometimento com intenção de defraudar ou com outro objetivo fraudulento. (BRASIL, 2023).

O artigo mencionado anteriormente aborda os crimes de falsificação informática cometido por meio eletrônico, contudo, a legislação brasileira já tipificava o crime de falsidade informática em seu artigo 3º da Lei nº 109/2009, preceituando a seguinte redação:

> [...] Quem, com intenção de provocar engano nas relações jurídicas, introduzir, modificar, apagar ou suprimir dados informáticos ou por qualquer outra forma interferir num tratamento informático de dados, produzindo dados ou documentos não genuínos, com a intenção de que estes sejam considerados ou utilizados para finalidades juridicamente relevantes como se o fossem, é punido com pena de prisão até 5 anos ou multa de 120 a 600 dias. (BRASIL, 2009).

O crime de falsidade informática resulta na alteração dos dados inseridos num sistema informático ou do tratamento por via do mesmo sistema, em que resulta na criação de documentos ou dados falsos, gerando insegurança e desconfiança nos documentos no tráfico jurídico-probatório. Diferente do que dispõe o 3º da Lei nº 109/2009, o artigo 7º (Título 2) do Decreto nº 11.491/2023, estabelece que, danificar ou obter informações de um sistema por meio da inserção, alteração, apagamento ou supressão, de forma dolosa e não autorizada, objetivando defraudar ou com outro objetivo fraudulento é tipificado como crime. Dando seguimento ao estudo, o artigo 8º (Título 2) do Decreto nº 11.491/2023 que dispõe sobre fraude informática, dispõe a seguinte redação:

> Cada Parte adotará medidas legislativas e outras providências necessárias para tipificar como crime, em sua legislação interna, a conduta de quem causar, de forma dolosa e não autorizada, prejuízo patrimonial a outrem por meio de: a. qualquer inserção, alteração, apagamento ou supressão de dados de computador; b. qualquer interferência no funcionamento de um computador ou de um sistema de computadores, realizada com a intenção fraudulenta de obter, para si ou para outrem, vantagem econômica ilícita. (BRASIL, 2023).

Ocorre que, a legislação brasileira em seu artigo 171, §2º-A do Código Penal trata sobre a fraude eletrônica, que ocorre se for cometida através de informações ditas pela vítima ou terceiro induzido, através de redes sociais ou outros meios fraudulentos análogos. Além disso, em seu §2-B, estabelece aumento de pena para quando o servidor utilizado estiver além do território nacional. Segue a redação do referido dispositivo:

> Art. 171 – [...] § 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo. [...] § 2º-B. A pena prevista no § 2º-A deste artigo, considerada a relevância do resultado gravoso, aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional [...]. (BRASIL, 1940).

Além disso, cabe mencionar a Lei nº 12.737/12, conhecida como Lei Carolina Dieckmann, prevê sanções penais para os crimes cometidos contra a privacidade na internet, como a exposição de conteúdos de natureza íntima sem consentimento. Outra importante legislação é a Lei Geral de Proteção de Dados (LGPD), que estabelece diretrizes para a proteção e o uso adequado de dados pessoais no Brasil. A LGPD prevê medidas protetivas que buscam evitar a exposição de informações confidenciais na rede, bem como a necessidade de consentimento explícito por parte dos usuários em relação à coleta e tratamento de dados.

Em suma, a legislação brasileira possui disposições que buscam coibir as fraudes eletrônicas e outros tipos de cibercrimes, estando em consonância com as disposições estabelecidas pela Convenção de Budapeste. A proteção da privacidade e segurança dos usuários da internet e o combate à criminalidade digital são fundamentais para a manutenção da confiança na rede e para a garantia dos direitos dos usuários.

Por fim, o artigo 9º (Título 3) do Decreto nº 11.491/2023, aborda sobre os crimes relacionados ao conteúdo da informação, especificamente sobre o crime de pornografia infantil, em que é tipificado condutas, cometidas dolosamente, a produção de pornografia infantil distribuída por meio de sistema de computador.

Fazendo ênfase a esse novo crime inserido pela Convenção de Budapeste, também vale mencionar os artigos 240 e 241 da Lei nº 11.829/2008 (Estatuto da Criança e do Adolescente), em que tipifica o crime de pornografia infantil. O artigo 240 do ECA é classificado como crime comum, assim, pode ser cometido por qualquer pessoa, além de ser considerado como crime formal, que independe de resultado naturalístico. Cabe ressaltar que esse artigo trata de crimes praticados por meio de computadores com acesso à internet, e lidera o número de denúncias, principalmente por lidar com vítimas tão vulneráveis, como crianças e adolescentes.

O Código Penal Brasileiro também prevê a penalização da produção, venda, exposição, distribuição, publicação, divulgação e armazenamento de material pornográfico envolvendo crianças e adolescentes, estipulando pena de reclusão de quatro a oito anos e multa. Além dessas legislações, o Brasil também é signatário da Convenção da Haia sobre os Aspectos Civis do Sequestro Internacional de Crianças, que estabelece a cooperação internacional para a proteção dos direitos da criança, incluindo medidas para prevenção e erradicação da exploração sexual de crianças.

Dessa forma, é possível concluir que a legislação brasileira está em conformidade com as exigências da Convenção de Budapeste no tocante à pornografia infantil, prevendo medidas rigorosas de proteção das crianças e adolescentes contra esse tipo de crime.

4.2 Adequação dos mecanismos de cooperação técnicas

O processo de adequação da Convenção sobre Cibercrime na legislação brasileira exigirá novos poderes e procedimentos para a obtenção de provas eletrônicas e prestação de assistência jurídica mútua entre os Estados-membros, não limitada a crimes cibernéticos. A Convenção de Budapeste foi promulgada no Brasil através do Decreto nº 11.491/2023, assim, segue a análise da introdução da cooperação internacional após a promulgação do referido decreto e a necessidade de harmonização com a legislação brasileira.

A legislação brasileira, estabelece na Constituição Federal de 1988 a competência dos órgãos que tratam acerca dos procedimentos de cooperação jurídica internacional. O Supremo Tribunal Federal é um órgão competente para tal assunto, podendo processar e julgar pedidos de extradição solicitados por Estados estrangeiros, assim segue o dispositivo: "Art. 102. Compete ao Supremo Tribunal Federal, precipuamente, a guarda da Constituição, cabendo-lhe: I - processar e julgar, originariamente:[...] g) a extradição solicitada por Estado estrangeiro [...]" (BRASIL, 1988).

Além disso, o Superior Tribunal de Justiça detém competência para a homologação de sentenças estrangeiras e a concessão de exequatur às cartas rogatórias, conforme artigo 105, inciso I, alínea "i" da Constituição Federal de 1988. Por fim, a Justiça Federal possui competência para a execução das cartas rogatórias após o exequatur, e a sentença estrangeira após homologação, assim dispõe o artigo 109, inciso X da Constituição Federal de 1988.

O artigo 733 do Código de Processo Penal trata dos instrumentos utilizados para comunicação entre autoridades nacionais e estrangeiras para a cooperação jurídica, assim, prevê a necessidade de sua remessa pelo juiz singular ao Ministro da Justiça, com o fito de dar cumprimento por via diplomática às autoridades estrangeiras competentes. Segue o artigo 733 do CPP, com a seguinte redação:

> O juiz, de ofício, ou a requerimento do interessado, do Ministério Público, ou do Conselho Penitenciário, julgará extinta a pena privativa de liberdade, se expirar o prazo do livramento sem revogação, ou na hipótese do artigo anterior, for o liberado absolvido por sentença irrecorrível. (BRASIL, 1941).

A Cooperação Direta entre as polícias é uma cooperação que não necessita da intervenção do Poder Judiciário para sua validade, no qual ocorre através do intercâmbio de informações policiais por meio da Interpol, em que consiste na atuação da autoridade nacional em busca de realizações de diligências investigativas no território nacional de um país estrangeiro, e vice-versa (COAF, 2020).

Vale ressaltar que, essa cooperação é coordenada pelo órgão da Polícia Federal, em que é feita dentro do território brasileiro, através da Coordenação-Geral de

Cooperação Internacional (CGCI), que opera dentro do Departamento de Polícia Federal. A cooperação possui atribuições como de intercâmbio de informações do mesmo gênero e organizações reconhecidas pelo Brasil, em que congregam organismos policiais ou demonstram interesses na investigação de crimes, assim, pode ser mencionado exemplos como a Interpol, Europol, Ameripol etc. (COAF, 2020).

Apesar de o Brasil caminhar no sentido de uma melhoria na cooperação jurídica internacional, o combate aos cribercrimes demonstra uma complexidade maior quando se trata de crimes que não respeitam as fronteiras, sendo necessário um auxílio maior entre os países para uma efetividade no enfrentamento à cibercriminalidade. Diante esse problema, o Brasil tornou-se país membro da Convenção de Budapeste, tratado internacional que uniformiza a forma como os Estados tratam do assunto.

A Convenção de Budapeste inclui mecanismos de cooperação técnica para os países-membros objetivando a prevenção dos crimes cibernéticos, tais quais: o estabelecimento de marcos legais para a prevenção e combate aos cibercrimes, definindo o conceito de cibercrimes e as sanções claras para este crime; a melhoria da capacidade de investigação e processo de crimes cibernéticos incluindo melhorias na capacitação de autoridades encarregadas da aplicação da lei e o desenvolvimento de estratégias para combater esses crimes; a cooperação internacional entre os países-membros em busca da prevenção dos crimes cibernéticos; e o fomento de inovações e tecnologias, para prevenir e reprimir os crimes cibernéticos.

4.3 Os possíveis problemas na adesão do Brasil à Convenção de Budapeste

A legislação brasileira no quesito combate aos cibercrimes e a cooperação internacional apresenta um grande atraso, pois não há lei nacional ou internacional que supra a necessidade no combate dos crimes virtuais, principalmente quando se aborda os temas de investigação e punição dos referidos crimes. A adesão do Brasil à Convenção de Budapeste foi o meio legal mais eficaz na identificação e punição dos cibercriminosos,

necessitando, assim, de algumas adequações legislativas para fazer parte dos países signatários desse tratado.

Inicialmente, a adesão do tratado internacional no ordenamento jurídico brasileiro foi considerada pelas autoridades governamentais uma grande conquista na luta contra os crimes virtuais, contudo, o processo de adesão também gerou grandes preocupações, qual seja: a celeridade no processo de adesão; a adesão total e irrestrita à Convenção de Budapeste; e por fim, a falta de uma lei geral de proteção de dados pessoais que aborde os temas de persecução penal e segurança pública.

Apesar da celeridade da adesão do tratado internacional na legislação brasileira, o tema foi discutido anteriormente por uma parcela da população, delimitando preocupações e falhas recorrentes no combate aos cribercrimes que deveriam ser consertadas. A Lei Geral de Proteção de Dados (LGPD) é uma legislação brasileira necessárias na prevenção do vazamento de dados pessoais, consequentemente podendo ser considerada como um meio de prevenção de crimes virtuais (DUARTE, 2022).

Apesar de as leis vigentes na legislação brasileiras demonstrarem ineficácia quanto aos crimes que ultrapassam as fronteiras internacionais, ressalta-se que estas estão dentro dos padrões internacionais criados pela Convenção de Budapeste, pois o referido tratado foi utilizado como guia na criação destas normas. Ademais, tendo em vista as poucas discussão e debates acerca do tratado internacional supramencionado, enfatizando as leis brasileiras e a adequação dos novos tipos penais inseridos pela Convenção, ainda poderá ser alvo de discussão mesmo após a promulgação do Decreto nº 11.491/2023, principalmente pelas autoridades nacionais como o Ministério Público em um processo democrático (DUARTE, 2022).

O segundo tema de pauta de discursão, aborda acerca da adesão total e irrestrita à Convenção de Budapeste no Brasil, no qual, o novo Decreto 11.491/2023 após a sua entrada em vigor necessitaria de adequações na legislação brasileira já vigente, ocasionando, consequentemente conflitos para as devidas mudanças. Contudo, o tratado internacional supramencionado busca harmonizar e estabelecer normas comuns para a

prevenção de crimes cibernéticos em todo o mundo, incluindo a proteção de dados pessoais.

Para evitar conflitos entre a Convenção de Budapeste e as leis nacionais, é importante que o Brasil adote medidas legais e institucionais após implementação da Convenção. Essas medidas incluem a criação de leis nacionais que estejam em conformidade com as normas estabelecidas na Convenção, a capacitação dos órgãos de fiscalização para lidar com questões relativas a crimes cibernéticos, e a adaptação de instâncias administrativas e judiciárias para tratar com os novos desafios provenientes do ambiente virtual.

Assim, a implementação da Convenção pode gerar conflitos de leis, contudo, esse conflito pode ser minimizado e controlado por meio de adoção de medidas legais e institucionais adequadas através da cooperação internacional. Apesar das preocupações acerca da adequação total e sem restrições ao tratado internacional, vale ressaltar que, durante o processo de adequação não ocorreu nenhum tipo de conflito significante entre a legislação brasileira e a Convenção de Budapeste, ou outro instrumento internacional de direitos humanos.

O terceiro tema causador de preocupação na adesão da Convenção de Budapeste à legislação brasileira é acerca da privacidade, devido a Convenção estabelecer a previsão de autorização para que as autoridades dos Estados-membros coletem, analisem e divulguem dados armazenados em sistemas informáticos para a prevenção e repressão de crimes cibernéticos. Diante disso, essa autorização pode levar a invasão de privacidade, especialmente se não houver mecanismos adequados de proteção de dados pessoais.

Assim, essa preocupação pode ser descartada e evitada caso utilize mecanismos de proteção de dados, tais como a anonimização de dados pessoais, em que busca resguardar os dados dos usuários, para fins de prevenção e repressão dos crimes cibernéticos; a criptografia de dados pessoais, dificultando o acesso às informações, resguardando a privacidade das pessoas e prevenindo a invasão indevida de sistemas informáticos; a regulação de acesso e compartilhamento de dados, estabelecendo limites claros e precisos

para a coleta; e por fim, o fortalecimento das instituições de proteção de dados, em busca de garantir o direito dos cidadãos.

5 CONSIDERAÇÕES FINAIS

Ao final deste estudo, torna-se evidente que a adesão do Brasil à Convenção de Budapeste marca um ponto de inflexão significativo na luta contra o cibercrime no cenário nacional e internacional. Essa conclusão é fruto de uma análise crítica e detalhada dos diversos aspectos envolvidos nesse processo.

Inicialmente, é imprescindível reconhecer que a legislação brasileira já possuía uma base sólida para o tratamento de delitos virtuais, alinhada, em grande medida, aos preceitos estabelecidos pela Convenção de Budapeste. No entanto, o Decreto nº 11.419 de 17 de abril de 2023 não se limita a uma mera formalidade. Ele introduz nuances cruciais, especialmente no que tange à cooperação jurídica internacional. Essa nova dimensão normativa promete superar as barreiras jurisdicionais e operacionais, permitindo um combate mais eficiente e coordenado contra o cibercrime.

É imperativo destacar que a natureza transnacional do cibercrime apresenta desafios singulares. Os criminosos digitais operam frequentemente além das fronteiras nacionais, explorando as lacunas legais e a fragmentação da aplicação da lei. Neste contexto, a Convenção de Budapeste surge como um catalisador para a cooperação internacional. A participação de organizações como a Interpol e a Europol é crucial nesse cenário, fornecendo uma plataforma robusta para troca de informações, investigações conjuntas e a formalização de acordos cooperativos entre nações. Essa abordagem colaborativa é fundamental para enfrentar a complexidade e a agilidade dos cibercriminosos.

A conclusão deste estudo não seria completa sem a proposição de recomendações estratégicas para o Brasil. A adesão à Convenção é um passo positivo, mas deve ser acompanhada por um investimento consistente em capacitação em segurança cibernética. O fortalecimento de parcerias público-privadas também se mostra essencial para uma

resposta eficaz e integrada ao cibercrime. O Brasil, ao abraçar essas estratégias, não apenas salvaguardará seus interesses nacionais, mas também contribuirá de maneira significativa para o esforço global de criar um ciberespaço mais seguro e resiliente.

Em suma, a Convenção de Budapeste representa um marco na legislação e cooperação internacional contra o cibercrime. O Brasil, ao integrar-se a esse tratado, posiciona-se de forma proativa no cenário global, adotando uma postura firme contra as ameaças digitais. Este estudo evidencia que, com as estratégias adequadas e a colaboração contínua entre nações, é possível enfrentar os desafios do cibercrime de maneira eficiente, promovendo um ambiente digital seguro para todos.

REFERÊNCIAS

BITENCOURT, Cezar. **Tratado de Direito Penal**. 10. ed. São Paulo: Saraiva, 2006.

BOITEUX, Luciana. Crimes informáticos: reflexões sobre a política criminal inseridas no contexto internacional atual. São Paulo: Revista dos Tribunais, 2004.

BRASIL. Constituição de 1988. Constituição da República Federativa do Brasil. **Diário Oficial [da] República Federativa do Brasil**, Poder Executivo, Brasília, DF, 5 out. 1988.

BRASIL. **Convenção sobre Cibercrime**. Budapeste: MPF, 2001.

BRASIL. Decreto nº 11.491, de 12 de abril de 2023. Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001. **Diário Oficial [da] República Federativa do Brasil**, Poder Executivo, Brasília, DF, 13 abr. 2023.

BRASIL. Decreto-Lei no 2.848, de 7 de Dezembro de 1940. Brasília, Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 20 out. 2023.

BRASIL. Decreto-Lei Nº 3.689, de 3 de Outubro de 1941. Brasília, Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 20 out. 2023.

BRASIL. Lei Complementar Nº 109, de 29 de Maio de 2001. Brasília, Disponível em: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp109.htm. Acesso em: 20 out. 2023.

BRASIL. **Lei Nº 11.829, de 25 de Novembro de 2008.** Brasília, Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11829.htm. Acesso em: 20 out. 2023.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. **Diário Oficial [da] República Federativa do Brasil**, Poder Executivo, Brasília, DF, 3 dez. 2012.

BRASIL. Lei Nº 13.709, de 14 de Agosto de 2018. Brasília, Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 20 out. 2023.

CASTRO, José Roberto Wanderley. **A tipicidade dos crimes cibernéticos no Direito Penal brasileiro**: um estudo sobre o impacto da Lei 12.737/2012 e a (des)construção de uma dogmática penal dos crimes cibernéticos. 2018. 231 f. Tese (Doutorado em Direito) – Programa de Pós-Graduação em Direito, Universidade Federal de Pernambuco, Recife, 2018.

COAF. **O que faz o Coaf?**. Brasília, DF: Coaf, 2020.

COLLI, Maciel. **Cibercrimes**: limites e perspectivas à investigação policial de crimes cibernéticos. Curitiba: Juruá, 2010.

DUARTE, Ana Luísa Vieira. **Análise do encaixe da convenção de Budapeste no ordenamento jurídico brasileiro**. 2022. 48 f. TCC (Graduação em Direito) – Programa de Graduação em Direito, Universidade de Brasília, Brasília, DF, 2022.

JUNQUEIRA, Gustavo Octaviano Diniz e VANZOLINI, Maria Patrícia. **Manual de direito penal brasileiro**. São Paulo: Saraiva, 2018.

MAGGIO, Vicente de Paula Rodrigues.Novo crime: invasão de dispositivo informático - CP, Art. 154-A. **Jusbrasil**, 2023. Disponível em: https://vicentemaggio.jusbrasil.com.br/. Acesso em: 7 mar. 2023.

MARQUES, Garcia; MARTINS, Lourenço. **Direito da Informática**. 2. ed. Coimbra: Almedina, 2006.

NICOLAI, Thiago; ALVEZ, Guilhrme Serapicos Rodrigues. O aumento silencioso dos cibercrimes. **Migalhas**, [*S.l.*], 2020. Disponível em: https://www.migalhas.com.br/depeso/326593/o-aumento-silencioso-dos-cibercrimes. Acesso em: 29 maio 2023.

NOGUEIRA, José Helano Matos. **Fundamentos de segurança cibernética**. Joinville: Clube de Autores, 2021.

SIMAS, Diana Viveiros de. **O cibercrime**. 2014. 170 f. Tese (Doutorado em Direito) – Programa de Pós-Graduação em Direito, Universidade Lusófona de Humanidades e Tecnologias, Lisboa, 2014.

VECCHIA, Evandro Dalla. **Perícia digital da investigação à análise forense**. Campinas: Millennium, 2020.

O *DATA* ATIVISMO EM PROL DA PROTEÇÃO AOS DIREITOS DA PERSONALIDADE NO CIBERESPAÇO

DATA ACTIVISM FOR THE PROTECTION OF PERSONAL RIGHTS IN CYBERSPACE

Ana Elisa Silva Fernandes Vieira[1]

Dirceu Pereira Siqueira[2]

RESUMO: Esta pesquisa tematiza a atuação dos movimentos sociais por meio do ciberativismo na defesa dos direitos da personalidade. Este estudo analisa a importância do data ativismo operado nas mídias sociais para a proteção dos direitos da personalidade. O problema de pesquisa pode ser sintetizado na questão: as formas de ativismo digital podem ser consideradas como mecanismos sociais para a proteção dos direitos da personalidade dos usuários nas redes sociais? O objetivo geral consiste em elucidar em que medida as práticas emergentes de ativismo de dados, que assumem uma postura crítica em relação à datificação e à coleta massiva de dados, relacionam-se à tutela dos direitos da personalidade humana. Utiliza do método dedutivo com a técnica de revisão bibliográfica em textos no tema. Conclui que o ativismo digital tensiona novos contextos de violações aos direitos da personalidade, e fomenta a articulação de práticas individuais e coletivas que questionam o uso desses atributos da personalidade no ciberespaço.

---

[1] Doutoranda em Ciências Jurídicas com ênfase em Direitos da Personalidade pela UNICESUMAR. Bolsista no Programa de Suporte à Pós-Graduação de Instituições de Ensino Particulares PROSUP/CAPES (módulo Bolsa) pelo Programa de Pós-Graduação em Ciências Jurídicas na UNICESUMAR. Membra do Grupo de Pesquisa do CNPq: "Políticas Públicas e Instrumentos Sociais de Efetivação dos Direitos da Personalidade". Mestre em Ciências Jurídicas com ênfase em Direitos da Personalidade pela UNICESUMAR. Graduada no Curso de Direito pela Pontifícia Universidade Católica do Paraná. Lattes: http://lattes.cnpq.br/4095037334203667. ORCID: https://orcid.org/0000-0002-0016-8829.

[2] Coordenador e Professor Permanente do Programa de Doutorado e Mestrado em Direito da Universidade Cesumar, Maringá, PR (UniCesumar); Pós-doutor em Direito pela Faculdade de Direito da Universidade de Coimbra (Portugal), Doutor e Mestre em Direito Constitucional pela Instituição Toledo de Ensino - ITE/Bauru, Especialista Lato Sensu em Direito Civil e Processual Civil pelo Centro Universitário de Rio Preto, Pesquisador Bolsista - Modalidade Produtividade em Pesquisa para Doutor - PPD - do Instituto Cesumar de Ciência, Tecnologia e Inovação (ICETI), Professor nos cursos de graduação em direito da Universidade de Araraquara (UNIARA) e do Centro Universitário Unifafibe (UNIFAFIBE), Professor Convidado do Programa de Mestrado University Missouri State – EUA, Editor da Revista Direitos Sociais e Políticas Públicas (Qualis B1), Consultor Jurídico, Parecerista, Advogado. Orcid: https://orcid.org/0000-0001-9073-7759. Lattes: http://lattes.cnpq.br/3134794995883683.

Palavras-chave: Ciberespaço; Data Ativismo; Direitos da Personalidade; Instrumentos de tutela.

ABSTRACT: This research focuses on the actions of social movements through cyberactivism in defense of personality rights. This study analyzes the importance of data activism operated on social media for the protection of personality rights. The research problem can be summarized in the question: can forms of digital activism be considered as social mechanisms for protecting the personality rights of users on social networks? The general objective is to elucidate the extent to which emerging practices of data activism, which take a critical stance in relation to datafication and massive data collection, are related to the protection of human personality rights. It uses the deductive method with the bibliographic review technique in texts on the topic. It concludes that digital activism tensions new contexts of violations of personality rights, and encourages the articulation of individual and collective practices that question the use of these personality attributes in cyberspace.

Keywords: Data Activism; Personality Rights; Guardianship instruments; Cyberspace.

1 INTRODUÇÃO

Contemporaneamente, têm surgido novas formas de mobilização coletiva e ativismo, com a utilização de mídias digitais como recursos para a participação política cívica. Paralelamente, o aumento do uso de plataformas de redes sociais, nas últimas décadas, ocasionou o advento e progresso de novas formas de comunicação na sociedade, e por consequência, de formas de se relacionar, seja com outras pessoas, seja com as empresas que ofertam os serviços e produtos utilizados. Nesse contexto, o Direito tem se preocupado em como essas mudanças impactam positiva e negativamente os direitos fundamentais e da personalidade dos cidadãos e usuários. Muitos são os casos de violações à vida privada, privacidade e dados pessoais, liberdade, honra, imagem e dentre outros, em que os elementos e expressões da personalidade são explorados e ameaçados.

Este artigo tematiza uma nova forma de ativismo para a tutela dos direitos da personalidade. Em particular, analisa o *data* ativismo que consiste em um novo campo de estudos e de manifestação na sociedade da informação, em que os dados remediam práticas de ativismo. Tratam-se de iniciativas que buscam interferir na *datificação*, ao contestar as relações de poder por meio da apropriação de práticas e infraestrutura de

dados

Nesse contexto, a problemática que orienta a investigação sintetiza-se no questionamento: as formas de ativismo digital podem ser consideradas como mecanismos sociais para a proteção dos direitos da personalidade dos usuários nas redes sociais? Procura-se compreender a noção de ativismo de dados como uma ferramenta de tutela e proteção aos direitos da personalidade, enfatizando o ativismo de dados como uma construção teórica que se encontra em evolução.

O objetivo geral consiste em elucidar em que medida as práticas emergentes de ativismo de dados, que assumem uma postura crítica em relação à *datificação* e à coleta massiva de dados, relacionam-se à tutela dos direitos da personalidade humana. Em outras palavras, se o *data* ativismo pode ser considerado um mecanismo de tutela e proteção dos direitos da personalidade no ciberespaço. Como desdobramento do objetivo geral, na primeira seção explora as noções de resistência, ativismo e o advento de um novo campo teórico chamado de ativismo digital ou data ativismo. Na segunda seção, analisa em que medida o *data* ativismo pode criar contextos de proteção e resguardo dos direitos da personalidade.

Como percurso metodológico para o desenvolvimento da pesquisa, utiliza o método de abordagem dedutivo, parte-se de tópicos e assuntos gerais para chegar a conclusões específicas no campo da efetividade dos direitos da personalidade, e como técnica de investigação e para fundamentar todos os objetivos propostos, emprega a revisão da literatura não sistemática

Ressalta-se que esta pesquisa não pretende esgotar a temática, mas busca-se relacionar os conceitos de ativismo digital e direitos da personalidade, e contribuir teoricamente para o avanço do conhecimento no campo da efetividade dos direitos da personalidade.

2 NOVAS FORMAS DE RESISTÊNCIA E ATIVISMO NO ESPAÇO DIGITAL

Na contemporaneidade, as tecnologias digitais, integradas no cotidiano social, revolucionaram a forma como as pessoas se comunicam e compartilham informações

(CAMPOS; PEREIRA; SIMÕES, 2016, p. 35). As plataformas de mídias sociais, definidas como "ferramentas online que dão suporte à interação social entre usuários" (HANSEN, SHNEIDERMAN, SMITH, 2011, p. 30), descortinam um novo sistema de comunicação capaz de abarcar e integrar todas as formas de expressão, bem como a diversidade de interesses, valores e de conflitos sociais (CASTELLS, 1999, p. 461).

Nesse contexto, as mídias digitais podem ser vistas sob duas perspectivas antagônicas: de modo otimista ou pessimista. No primeiro, enfatiza-se características da diminuição do custo de se comunicar, a velocidade com que a informação viaja, a eliminação da distância física, a horizontalidade da comunicação (JENKINGS, 2008). No segundo, pessimista, destaca-se o empobrecimento do debate político com discussões predominando a simplificação, o uso de conteúdo desinformativo como estratégia de reafirmação de ideologias e a perda de privacidade no ciberespaço (CAVALCANTI; JARDELINO; NASCIMENTO, 2020, p. 42558). Desse modo, é possível afirmar que a digitalização tem impactado e influenciado diversas esferas da sociedade, como o trabalho, as relações sociais, o lazer e até mesmo as formas de ativismo (CAMPOS; PEREIRA; SIMÕES, 2016, p. 35).

Os movimentos sociais de ativismo buscam redefinir a esfera pública por meio de conglomerados e parcerias com entidades civis e sociedade civil, para a construção de inovações sociais e gerar saberes na sociedade (REIS; OLIVEIRA, 2017, p. 49). Para Milan e Van Der Velden (2016, p. 66), a noção de ativismo abrange práticas de resistência e instâncias de apropriação como meios distintos, porém complementares para alcançar objetivos políticos e a coexistência de atitudes em relação às instituições e às normas sociais.

Segundo Fonseca (2014, p. 61) "todo ato de ativismo social é resultado de uma insatisfação ou necessidade de expressão individual ou coletiva, com o intuito de dar visibilidade a uma causa" específica. Inclusive, na sociologia, o debate sobre a ascensão de formas de ativismo e descentralização política, considera tais movimentos como mecanismos de empoderamento da sociedade civil e fortalecimento da participação e da cidadania (DESLANDES, 2018, p. 3133).

A internet desponta como uma ferramenta aos movimentos sociais pois torna possível a rápida divulgação de conteúdos e a comunicação em larga escala (CAMPOS; PEREIRA; SIMÕES, 2016, p. 30). Mas não apenas isso. Atualmente, as próprias tecnologias de informação tornam-se uma causa de contestação social, constituindo a razão central de certos movimentos sociais, como por exemplo, contra a censura digital e a favor da liberdade de expressão (CAMPOS; PEREIRA; SIMÕES, 2016, p. 30).

Em outras palavras, consiste também em uma área sensível e de conflito que leva os indivíduos a terem um conjunto de motivações para a ação política cívica tendo internet por objeto dessa disputa. Tais conflitos são levados a cabo por um conjunto de mobilizações sociais que propõem formas tecnológicas de transformação social (CAMPOS; PEREIRA; SIMÕES, 2016, p. 32). Exemplificando, há movimentos que promovem o combate à exclusão digital por meio da uma nova infraestrutura tecnológica e da promoção de uma literacia digital emancipatória, movimentos que combatem a *cibercensura* promovem a privacidade, liberdade de expressão e transparência (MOREIRA, 2022; SIQUEIRA, MOREIRA; VIEIRA, 2023).

Nesse cenário é que surge o conceito de *ciberativismo*, o qual refere-se à utilização do espaço digital para movimentos e discursos sociais (REIS; OLIVEIRA, 2017, p. 48). Segundo Fonseca (2009, p. 65) *ciberativismo* ou o ativismo digital está relacionado com "a militância exercida através das tecnologias digitais e da internet, presentes no mundo *ciberespacial*". Exemplificando, há movimentos sociais, ONGs e outros grupos da sociedade civil que vêm se apropriando do ciberespaço como arena de ativismo (MEDEIROS; LORDÊLO, 2012, 113).

Especificamente no Brasil os casos de *ciberativismo* são variados, com as redes sociais virtuais em ênfase num continente que enfrenta partidos políticos fragilizados e desigualdade social. É possível destacar o Avaaz, as Manifestações de junho 2013, a "Mídia Ninja", o "Movimento Brasil Livre" (MBL) e o "Vem pra Rua" (VPR) (CAVALCANTI; JARDELINO; NASCIMENTO, 2020). Vale ressaltar, porém, que o ativismo digital necessariamente baseia-se em uma ideologia política (de esquerda ou direita), pois a luta por liberdades individuais, pode ser identificada em ambas, "ao se

contrapor a sistemas ditatoriais, abusos de autoridade em democracias, denúncias de corrupção estatal, sem que necessariamente exista uma adesão a um libertarianismo ou a um socialismo em particular" (VASCONCELOS FILHO; COUTINHO, 2016, p. 23).

O uso instrumental da internet, enquanto ferramenta a serviço dos movimentos sociais pode ser visualizado desde a simples postagem de informações em sites, blogues ou páginas de redes sociais, ou até a usos mais sofisticados (RODRIGUEZ; ROIG, 2004). Estes diferentes níveis pressupõem autores diferenciados, dotados de níveis de conhecimento distintos e de intenções variadas (CAMPOS; PEREIRA; SIMÕES, 2016, p. 30).

Na contemporaneidade, então, o ciberespaço tem sido utilizado, como um ecossistema para a atuação de atores sociais e ativistas, discussão e manifestação em defesa de causas específicas. Segundo Lemos (2009), a nova lógica comunicacional abriga um sistema em que todos os participantes da interação podem comunicar uns aos outros, criando um modelo multidirecional em oposição ao padrão anterior, da *mass media* unidirecional. Para Raminelli et al (2011, p.2) há no *ciberativismo* um caráter democrático, pois através dele os cidadãos podem ter "vez e voz". Sendo assim, é possível afirmar que as tecnologias digitais expandem os contextos de comunicação e de expressões de resistência na sociedade, na medida em que amplia as condições e possibilidades de acesso à informação. Logo, na atualidade, os locais de ativismo podem ser concebidos como espaços híbridos (CASTELLS, 2003).

Em relação à atuação dos movimentos sociais na internet, segundo Castells (2003, p. 115), a internet é um instrumento útil a ser usado que se ajusta às características básicas do tipo e movimento social surgindo em determinada sociedade. O autor elenca algumas das características dos movimentos sociais da atualidade, como o fato de serem desencadeados por uma centelha de indignação, a ausência de uma liderança específica, a profundidade da reflexão e o não pragmatismo, e estão voltados para a mudança nos valores da sociedade, sendo políticos em um sentido fundamental (CASTELLS, 2013, p. 159-165).

Moraes (2007, p. 1) explica que a internet pode ser entendida como um ecossistema digital caracterizado por uma arquitetura descentralizada, que multiplica as fontes de emissão, disponibilização ininterrupta de informações e dados, e possibilita a interação entre indivíduos. Ademais, explica Lima (2012, p. 74) que "o ativismo digital pode se basear principalmente no reforço dos valores culturais de determinado grupo, em detrimento de uma reavaliação dos mesmos".

A partir do desenvolvimento por Vegh (2003, p. 72-73) é possível classificar o ativismo online em três categorias principais: de conscientização e apoio; de organização e mobilização; e de ação e reação. A categoria de conscientização e apoio consiste no ativismo estruturado como fonte de informação, e que objetiva conscientizar os internautas a respeito das causas defendidas. Nesse caso, os discursos são disseminados em sites, comunidades virtuais, blogs, perfis em redes sociais, como forma de buscar o apoio para as causas ao permitir que tais plataformas digitais propaguem os discursos comumente negligenciados pela mídia de massa e os veículos tradicionais de comunicação (LIMA, 2012, p. 82-86).

A segunda categoria, denominada de organização e mobilização, é desenvolvida de três formas: organização offline para mobilização/ação também offline, mas que gera resultado mais eficaz em ambiente online; organização online para ação offline; e organização e mobilização exclusivamente online (LIMA, 2012, p. 82-86; REIS; OLIVEIRA, 2017, p. 49). Para Santos (2011, p. 3), estes movimentos se articulam com o intuito de "alcançar suas tradicionais metas ou lutar contra injustiças que ocorrem na própria rede". Por fim, a terceira e última categoria, ação e reação, é caracterizada pelo *hacktivismo*, ou seja, o ativismo praticado por hackers que consiste em ações invasivas a sites, bem como protestos ao ciberterrorismo (VEGH, 2003, p. 75).

Tal como a internet, a *datificação* tornou-se tanto um discurso quanto uma ferramenta (ou agente) para luta política (BERALDO; MILAN, 2019, p. 2). Milan e Van Der Velden (2016) propõem o conceito de "data ativismo", isto é, um conhecimento que escape à reificação do futuro, a partir de um desenvolvimento crítico da ciência e da tecnologia, inscrito pelo próprio uso dos dados pelos investigadores. O data ativismo ou

ativismo de dados é um campo de estudos em que os dados remediam o ativismo. O ativismo de dados propõe uma relação crítica com e em relação aos dados (BERALDO; MILAN, 2019, p. 3).

O ativismo de dados é uma das variações da ampla categoria de ativismo cibernético ou digital, como também é o *hacktivismo* (MILAN; VAN DER VELDEN, 2016, p. 60). Mas, para além do uso politicamente motivado de conhecimentos técnicos, o ativismo de dados é uma variação mais ampla e que ultrapassa o envolvimento com a infraestrutura e abrange a informação e o conhecimento como uma categoria mais ampla de intervenção (MILAN; VAN DER VELDEN, 2016, p. 61).

O ativismo de dados é definido como uma "série de práticas sociotécnicas que, emergindo à margem da ecologia do ativismo contemporâneo, interrogam criticamente a *datificação* e suas consequências sociopolíticas" (COTÉ; GERBAUDO; PYBUS, 2016, p. 11). Segundo Ruppertetal (2017), ao buscar-se compreender a relação entre dados, ativismo e política, preocupa-se "não apenas com as lutas políticas em torno da coleta e implantação de dados, mas como os dados são geradores de novas formas de relações de poder e políticas em escalas diferentes e interconectadas". Sendo assim, o *data* ativismo ou ativismo de dados, reproduz-se em razão dos atuais mecanismos de dominação que se pautam na dinâmica capitalista de monetização dos dados digitais e *datificação* e têm sido constantemente tensionados pelos próprios agentes sociais e usuários, tendo em vista que a crescente disponibilidade dos dados é considerada como uma oportunidade sem precedentes para provocar mudanças sociais, positiva ou negativas (SOARES, 2018, 153).

Desse modo, o ativismo de dados é uma forma de manifestação na sociedade da informação, que se envolve com as novas formas que a informação, e a produção do conhecimento assumem na era da *datificação* (MILAN; VAN DER VELDEN, 2016, p. 61). Nesse contexto, Milan e Gutiérrez (2015, p. 123), explicam que o ativismo de dados "sinaliza uma mudança de perspectiva e atitude em relação à recolha massiva de dados que emerge no núcleo da sociedade civil". Nesse viés, o "data ativismo" apoia a emergência de novas culturas epistêmicas que "desafiam as leituras predominantes da

realidade" e "moldam a forma como relacionamo-nos com o conhecimento e sua validação" (MILAN; VAN DER VELDEN, 2016, p. 63).

No contexto desta investigação, o ativismo de dados trata-se de iniciativas que buscam interferir na *datificação*, contestando as relações de poder e narrativas existentes e/ou reapropriando práticas e infraestrutura de dados para fins distintos dos pretendidos e conhecidos pelos usuários e titulares. Essas iniciativas podem variar em escala, formas organizacionais, táticas, valores políticos, imaginários sociotécnicos. Apesar disso, o que todos elas compartilham é o papel central dos dados como mediadores e o objetivo do conflito e meios que possibilitam um repertório de ação (BERALDO; MILÃO, 2019, p. 2).

Milan e Van Der Velden (2016) abordam diferentes formas de ativismo que tornam os dados um novo tema de conflito, e destacam diferentes campanhas e movimentos sociais que discutem a questão do *big data*. Para tais movimentos, o *big data* tende a ser entendido como uma ameaça aos direitos individuais e de personalidade, em particular à privacidade. Para outros, porém, o *big data* pode ser encarado de modo positivo, ao permitir novas oportunidades de mudança social. Assim, o ativismo orientado a dados mobiliza práticas de dados para uma variedade de objetivos sociais, políticos ou pessoais (BERALDO; MILAN, 2019, p. 6).

Ressalta-se que por muitos anos a internet foi considerada como um espaço no qual não haveria ingerência nem dominação, e os usuários poderiam acessar os conteúdos livremente. Porém, ao descobrir as possibilidades de ação que a coleta e os tratamentos de informações que identificam ou possam identificar o usuário titular (dados pessoais), podem representar economicamente (ZUBOFF, 2020), a internet tornou-se um espaço através do qual governos e empresas começaram a recolher, armazenar, recuperar, analisar e apresentar dados que registram o que as pessoas fazem e dizem na Internet (RUPPERT; ISIN; BIGO, 2017).

A expressão em inglês "*datafication*" foi primeiro citada por Mayer-Schönberger e Cukier, na obra "*A Revolution That Will Transform How We Live, Work and Think*", em que a definiram como uma forma de quantificação que viabiliza a tabulação e análise

de informações, possibilitando que aspectos da vida humana possam ser processados por meios de formas de análise que são suscetíveis à automatização (MAYER-SCHÖNBERGER; CUKIER, 2013). Assim, a *datificação* é "um fenômeno contemporâneo, que se refere à quantificação da vida humana" por meio dos sistemas de informação. Em outras palavras, renderizar aspectos da vida humana em dados digitais (MEJIAS; COULDRY, 2019).

O tratamento de dados pessoais é utilizado para designar as operações técnicas que podem ser efetuadas sobre os dados pessoais, de modo informatizado ou não, com a finalidade de se refinar a informação, tornando-a mais valiosa e útil (MENDES, 2008, p. 72). Sendo assim, esse tratamento é dinâmico, pois consiste na ação de manejar a informação, relacionando e reelaborando dados, com intuito de se obterem conclusões a partir da aplicação de critérios (MENDES, 2008, p. 73). Os dados geralmente são organizados na forma de "banco de dados", um conjunto organizado e lógico de dados (MENDES, 2008, p. 73; McKelvey, 2014, p. 598), e são tratados em algoritmos que traçam o perfil dos usuários com base em seu comportamento e selecionam, classificam e personalizam o conteúdo de acordo com os dados do usuário (MILÃO, 2015, p. 3).

Esses algoritmos são denominados de opacos pois as operações são proprietárias e não divulgadas pelas plataformas (TUFEKCI, 2014). A *datificação* tem o potencial de alterar "as condições sob as quais podemos dar sentido ao nosso mundo e as nossas próprias ações", afetando "a nossa capacidade de agir com agência" (BAACK, 2015, p. 1). Ademais, segundo Rob Kitchin (2014, p. 2), a *datificação* têm consequências epistemológicas e afeta "a forma como o conhecimento é produzido, os negócios são conduzidos e a governação é implementada".

Beraldo e Milan (2019, p. 3), ao analisar as consequências da *datificação* sobre as pessoas concluem que elas são numerosas e diversas, e podem impulsionar a vigilância governamental, a definição de perfis empresariais, a discriminação algorítmica (HOFFMANN, 2019), com discussões sobre o colonialismo de dados (COULDRY; MEJIAS, 2018) e o capitalismo de plataforma (ZUBOFF, 2020). Estes processos,

explicam os autores, ocorrem tanto em regimes autoritários como em regimes liberais e tornam visível a reavaliação das relações de poder promovida pela *datificação.*

Nesse cenário, o ativismo de dados identifica-se como uma resposta popular ao aspecto crítico da *datificação*, em que se adota uma variedade de ações e repertórios, incluindo defesa de direitos, promoção da alfabetização, desenvolvimento de software e campanhas (BERALDO; MILAN, 2019, p. 6). Algumas das iniciativas existentes de ativismo de dados assumem a forma de atos individuais de resistência, enquanto outras consistem em mobilizações coletivas em grande escala" (BERALDO; MILAN, 2019, p. 7). A título de exemplo, cita-se as atividades promovidas por organizações de direitos digitais, instrutores de segurança e iniciativas de transparência algorítmica (BERALDO; MILAN, 2019, p. 6).

Esta pesquisa pretende avançar teoricamente ao demonstrar que é possível considerar as plataformas de mídias sociais como um instrumento do ativismo digital quanto o reconhecimento dessas plataformas como um novo tema de conflito nos discursos, relaciona-se a efetividade dos direitos da personalidade e a tutela da personalidade humana.

3 A TUTELA DA PERSONALIDADE HUMANA E DOS DIREITOS DA PERSONALIDADE POR MEIO DO DATA ATIVISMO

No decorrer do século XX, a revolução tecnológica modificou o sentido e o alcance dos direitos da personalidade exercidos no espaço digital. A título de exemplo, o direito à privacidade que antes era considerado de forma eminentemente negativa, adotou um sentido positivo como pressuposto para o reconhecimento de outros direitos fundamentais. Assim, esse direito da personalidade evoluiu para se adaptar às novas transformações sociais geradas pela revolução da tecnologia da informação. Além de adquirir um caráter positivo e de ser reconhecido no âmbito internacional, a privacidade foi reinterpretada para ensejar a proteção de dados pessoais, que passou a ser tutelada em ordenamentos jurídicos de muitos países ao entenderem que os dados constituem uma

projeção da personalidade do indivíduo, logo, sua proteção também tutela a personalidade e a dignidade do indivíduo por meio dos dados pessoais (MENDES, 2008, p. 18).

As primeiras tendências interpretativas dos tribunais brasileiros não tutelavam os dados em si, mas a comunicação desses dados, sob o fundamento do artigo 5º, XII do texto constitucional (CAMARA, 2010, p. 30-32). Sendo assim, entendia-se que a tutela não recaía sobre o dado, mas sobre a comunicação dele à terceiros, sendo que o controle da circulação de informações pessoais era instrumentalizado por meio do *habeas data*

Mais recentemente, porém, a doutrina reconheceu uma relação entre os dados pessoais e a identidade pessoal, passando a considerar o dado pessoal como um elemento afirmador da personalidade. Em outras palavras, elementos da própria personalidade individual. Assim, a personalidade humana passou a ser considerada como um bem da vida a ser tutelado pelo direito com a doutrina dos direitos da personalidade que teve o seu desenvolvimento em tempos recentes nas doutrinas germânicas e francesas, durante os séculos XIX e XX, quando a categoria dos direitos da personalidade esteve no centro de intensos debates doutrinários (QUEIROZ; ZANINI, 2021, p. 16).

Com o fim das duas Guerras Mundiais que assolou a Europa, os países passaram a se preocupar em encontrar meios jurídicos para assegurar que a pessoa humana não passasse mais por situações de despersonalização, tais como as vivenciadas pelos judeus nos campos de concentração. Ademais, as atrocidades cometidas durante as guerras evidenciaram que o pensamento liberal dos séculos XVIII e XIX, consubstanciado no Código Civil positivista clássico, no individualismo e no patrimonialismo, não tutelam a pessoa adequadamente (IKEDA; TEIXEIRA, 2022, p. 2360). Paulatinamente, os Estados Liberais preocupados com a igualdade formal do indivíduo e propriedade privada, adotaram elementos de um Estado Social que se preocupa com a igualdade material e a efetividade dos direitos.

As bases jurídicas foram reestruturadas para que o Estado cumprisse com essa nova posição, e foram estabelecidos direitos inatos que assegurem que as pessoas não sofram abusos, decorrentes do reconhecimento como ser humano. Tais direitos foram denominados de direitos humanos. Os direitos humanos, ao fazerem parte das

Constituições nacionais, foram chamados de direitos fundamentais, e visavam proteger a pessoa contra as arbitrariedades do Estado. Nas relações privadas, aqueles direitos voltados para a tutela da pessoa nas relações privadas, foram chamados de direitos da personalidade. Desse modo, os direitos da personalidade passaram a ter proeminência nos ordenamentos jurídicos, em decorrência do desenvolvimento dos direitos humanos e fundamentais.

Na Alemanha, tornou-se famosa a expressão "direitos de personalidade" cunhada por Gierke (1841-1921), responsável pelo aprofundamento da noção do direito geral da personalidade, a partir das premissas kantianas da pessoa (AMARAL, 2008, p. 288). Assim, segundo entendia o jurista alemão, esses seriam direitos que assegurariam ao sujeito um domínio sobre uma parte de sua própria personalidade (GOMES, 1966, p. 41).

Em relação à previsão dos direitos da personalidade, Queiroz e Zanini (2021, p. 17) explicam que surgiram dois grandes posicionamentos doutrinários. De um lado, defendia-se a tipificação fracionada dos direitos da personalidade em direitos subjetivos específicos, incidindo sobre aspectos particulares da personalidade. Por outro lado, considerava-se insuficiente a proteção da pessoa humana por meio de direitos tipificados, sendo necessária uma regra geral unitária, um direito geral de personalidade que compreendesse todos os casos relacionados aos bens da personalidade. Essa doutrina, promovida por Gierke, desenvolveu-se principalmente na Alemanha (GOMES, 1966; QUEIROZ; ZANINI, 2021).

A experiência brasileira quanto aos direitos da personalidade tem início no período colonial, quando o Código Civil português, influenciado pelas evoluções teóricas das demais nações, passou a prever a tutela da pessoa por meio de direitos típicos de personalidade e por uma cláusula geral. O primeiro Código Civil brasileiro, de 1916, inspirado na codificação alemã do BGB, não encontrou uma base estrutural para o resguardo amplo da pessoa; ao contrário, centralizava-se em interesses da pessoa proprietária (ASCENSÃO, 2014, p. 4; AMARAL, 1994, p. 236-237). Apesar disso, os direitos da personalidade já haviam sido versados pela doutrina brasileira (ANDRADE, 2013, p. 84).

É pacífica a compreensão na doutrina de que os direitos da personalidade, no Brasil, tiveram seu reconhecimento, enquanto categoria específica, em tempos recentes, se comparado aos países europeus. Foi somente com o advento da Constituição Federal de 1988, que o ordenamento jurídico brasileiro se estabeleceu sobre uma nova tábua de valores que influenciou a constitucionalização do Direito Civil, e por consequência, ampliou o espaço dos direitos da personalidade, seguindo o modelo de redemocratização e personalização ocidental (GOMES, 1966, p. 57). O Código Civil de 2002, influenciado pela então Constituição, deixou de ter como fundamentos o patrimonialismo e o individualismo do período industrial, para lançar-se à efetivação de valores existenciais e de justiça social (IKEDA; TEIXEIRA, 2022, p. 2361-2362). A lei civil, influenciada pelas legislações estrangeiras, trouxe em seu bojo um capítulo específico sobre o tema (artigos 11 a 21 do "CAPÍTULO II - Dos Direitos da Personalidade" da Parte Geral), com a previsão de direitos específicos, como o direito à vida, integridade, igualdade, honra, imagem e vida privada.

Em relação a conceituação dos direitos da personalidade, Tepedino (2004, p. 24) conceitua-os como direitos "atinentes à tutela da pessoa humana, considerados essenciais à sua dignidade e integridade". Bittar (2008) entende os direitos da personalidade como aqueles direitos reconhecidos à pessoa em suas projeções na sociedade, para a defesa de valores intrínsecos à humanidade, como a vida, a higidez e integridade física e psíquica, a intimidade, a honra, imagem etc. Freire de Sá e Moreira (2015, p. 47) compreendem os direitos da personalidade como "aqueles que têm por objeto os diversos aspectos da pessoa humana, caracterizando-a em sua individualidade e servindo de base para o exercício de uma vida digna".

A partir dessas definições, é possível concluir que o objeto de tutela dos direitos da personalidade são os atributos da personalidade que identificam o ser humano como pessoa; são os prolongamentos da individualidade humana considerados elementos fundamentais para o desenvolvimento da pessoa; os atributos humanos fundamentais que qualificam a pessoa. Os bens jurídicos tutelados tratam-se de "bens constituídos por determinados atributos ou qualidades, físicas ou morais, do homem, individualizado pelo

ordenamento jurídico" (LIMONGI FRANÇA, 1980, p. 145; SZANIAWSKI, 2005, p. 87). Sendo assim, o objeto de tutela dos direitos da personalidade refere-se às projeções físicas ou psíquicas da pessoa, ou as suas características mais importantes dessas projeções que identificam a pessoa como ela é (BORGES, 2007, p. 20; GOMES, 1966, p. 41).

A personalidade "traduz o conjunto de características e atributos da pessoa humana, considerada como objeto de proteção prioritária pelo ordenamento, sendo peculiar, portanto, à pessoa natural" (TEPEDINO, 2022, p. 193). Embora relacionados ao titular, esses direitos devem ser entendidos como pertencentes ao indivíduo incluídos na comunidade na qual vive, isto é, como instrumentos para realização da sociedade, e não concebidos de forma individualista (PERLINGIERI, 1999, p. 38).

No Direito Brasileiro, existem tanto os direitos da personalidade previstos expressamente nos artigos 12 em diante do Código Civil, quanto aqueles no art. 5º da Constituição Federal, como por exemplo o direito à imagem, honra, integridade física e disposição do próprio corpo, nome e vida privada (SZANIAWSKI, 2005, p. 136-137). Em paralelo, há uma cláusula geral de tutela da personalidade humana que reconhece a existência do direito geral de personalidade, um direito-fonte que funciona como fundamento para que novos direitos da personalidade sejam admitidos ou reinterpretados no sistema jurídico brasileiro (QUEIROZ; ZANINI, 2021, p. 29). Existindo um direito da personalidade expresso que reclame aplicação a determinado caso concreto, não se incide o direito geral da personalidade.

Apenas em caso de lesão à personalidade não tipicamente regulada, incide em toda sua plenitude o direito geral da personalidade, de modo a ampliar a tutela em novas expressões da personalidade. Assim, "sua aplicação se dá de forma subsidiária aos direitos especiais da personalidade, sendo englobante destes que, por seu turno, não esgotam o bem geral da personalidade" (QUEIROZ; ZANINI, 2021, p. 30).

Ressalta-se que a ausência de uma previsão expressa de uma cláusula geral de tutela da personalidade humana não deve ser supervalorizada, devido a possibilidade do reconhecimento de forma implícita, em decorrência do texto constitucional (QUEIROZ;

ZANINI, 2021, p. 32). Inclusive, Segundo Moraes (2006, p. 51), não há mais "que se discutir sobre uma enumeração taxativa ou exemplificativa dos direitos da personalidade, porque se está em presença, a partir do princípio constitucional da dignidade, de uma cláusula geral de tutela da pessoa". Sendo assim, o direito geral de personalidade está implícito no ordenamento jurídico brasileiro e se sustenta no princípio da dignidade da pessoa humana (art. 1º, III da CF), na permissão constitucional do reconhecimento de outros direitos e garantias fundamentais (art. 5º, parágrafo segundo da Constituição) e no art. 12 do Código Civil de 2002.

A garantia de que tais direitos não sejam taxativos e novas proteções sejam reconhecidas decorre da essencialidade que os direitos da personalidade possuem, segundo a qual os direitos da personalidade são imprescindíveis à personalidade. Nesse sentido, afirma Pontes de Miranda (2012, p. 69) que os direitos da personalidade "são todos os direitos necessários à realização da personalidade, à sua inserção nas relações jurídicas". De Cupis (2008, p. 24) explica que estes são direitos sem os quais a personalidade humana estaria completamente irrealizada, privada de todo o valor concreto, constituem a medula da personalidade. Devido a essa essencialidade é que novos direitos da personalidade podem (e devem) ser reconhecidos frente às novas demandas e ameaças na sociedade e a garantia de maior proteção aos indivíduos (JABORANDY; GOLDHAR, 2018, p. 487).

Nesse contexto, sendo possível a ampliação dos direitos da personalidade, em virtude da identificação de novos atributos ou expressões da personalidade humana, em especial na sociedade tecnológica, Saldanha (2021) defende a tese de que os dados pessoais tratam-se de uma quarta expressão dos direitos de personalidade humana, sendo portanto, merecedor de proteção específica, por um direito da personalidade específico: a proteção dos dados pessoais. Sendo assim, não é suficiente para o resguardo da pessoa uma proteção restrita apenas à comunicação dos dados. Sendo assim, entende-se que o próprio dado é merecedor de tutela na medida em que é um elemento da personalidade humana.

Segundo Wacks (1989, p. 25), "dado" pode ser compreendido como a informação em potencial, isto é, ele pode se transformar em informação se for comunicado, recebido e compreendido. Se o dado assume a forma de uma palavra impressa ele é imediatamente compreendido como informação pelo leitor. Mas, se o dado consiste em atos ou sinais que requeiram a interpretação antes de adquirirem qualquer sentido, ele permanece no estado de pré-informação até poder ser efetivamente compreendido por alguém (WACKS, 1989, p. 25).

Quanto ao conceito de dados pessoais, trata-se de fatos, comunicações e ações que se referem a circunstâncias pessoais ou materiais de um indivíduo identificado ou identificável. De acordo com a Diretiva Europeia 95/46/CE, o artigo 2º define que dados pessoais constituem "qualquer informação relativa a uma pessoa singular identificado ou identificável". O dispositivo prescreve que "é considerado identificável todo aquele que possa ser identificado, direta ou indiretamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social". Tais informações merecem tutela jurídica, uma vez que, por terem como objeto a própria pessoa, constituem um atributo de sua personalidade; tal tutela visa à proteção da pessoa e de sua personalidade e não dos dados per se (MENDES, 2008, p. 71).

Acontece que na atualidade, "os dados tornaram-se uma questão social e política não só porque dizem respeito a qualquer pessoa que esteja ligada à Internet, mas também porque reconfiguram as relações entre Estados e cidadãos" (RUPPERT; ISIN; BIGO, 2017, p. 1), devido aos efeitos da *datificação.* Isto porque, o potencial de uso dos dados ampliou-se, tornando-se um instrumento útil a modulação das relações sociais, preferências e oportunidades de vida, e das próprias democracias (RUPPERT, ISIN, BIGO, 2017, p. 2). De acordo com Tufekci (2014), as tecnologias digitais:

> [...] deram origem a uma nova combinação de *big data* e práticas computacionais que permitem a coleta massiva e latente de dados e a modelagem computacional sofisticada, aumentando a capacidade daqueles com recursos e acesso para usar essas ferramentas para transportar realizar

> campanhas de persuasão e engenharia social altamente eficazes, opacas e irresponsáveis nas esferas política, cívica e comercial.

Segundo explica Doneda (2021), o aumento exponencial no volume, na intensidade e mesmo na complexidade da temática dos dados pessoais fez com que fossem incorporados novos elementos para garantir a tutela integral da pessoa e o fortalecimento dos direitos individuais. Assim, a tese da proteção de dados pessoais começou a se estruturar com maior autonomia quando o processamento automatizado de dados passou a representar, por si só, um fator de risco para o indivíduo. Além disso, diferentemente de outras épocas, nas quais os mecanismos de imposição de poder eram a força e a coerção, os agentes interessados no poder na sociedade contemporânea utilizam-se da persuasão sobre os indivíduos, compondo um cenário social programado a partir do uso de tecnologias de dados (MOSTAFA; CRUZ; AMORIM, 2015, p. 361).

O debate em torno da política de dados não se limita apenas a analisar as lutas políticas em torno da recolha de dados, sua implantação e as formas de resistência às ameaças percebidas de coleta massiva de dados, por meio de soluções técnicas (BERALDO; MILAN, 2019, p. 4). Mas, amplia-se em elucidar "a forma como os dados são geradores de novas formas de relações de poder e de política em escalas diferentes e interligadas" (RUPPERT; ISIN; BIGO, 2017, p. 2). Assim, o ativismo de dados se destaca frente a demais movimentos sociais contemporâneos na medida em que trata o *big data* simultaneamente como ferramenta e fim da luta (MILAN, 2017, p. 3).

Além de analisar o fenômeno em si, nesta investigação procura-se considerar o *data* ativismo como uma forma de resistência, o contrapoder da era digital, segundo Castells (2015) ou, no dizer de Deleuze, "novas armas", nas atuais "sociedades de controle que estão substituindo as sociedades disciplinares" (DELEUZE, 1992, p. 219).

A partir dessas considerações, entende-se ser possível relacionar a política de dados como os direitos da personalidade em alguns aspectos. O ativismo de dados tensiona novos contextos de disputas e discursos frente a violações aos direitos da personalidade, e fomenta a articulação de práticas individuais e coletivas que questionam o uso desses atributos da personalidade no ciberespaço.

O ativismo digital também se vincula à liberdade, a partir do raciocínio foucaultiano sobre a liberdade conter condições de resistência. Ademais, o ativismo digital também com a liberdade, que é um direito da personalidade em espécie. A liberdade, segundo Foucault, que a considera como resistência ao poder, que não se confunde com o poder estatal, e não está estabelecido em um lugar propriamente dito, mas é exercido a partir de uma rede de incidência de poderes (FOUCAULT, 1988, p. 89). Foucault identifica duas formas de atuação desse poder: o poder disciplinar e o biopoder. Atualmente, porém, é possível refletir sobre a existência de uma nova forma de poder operada por meio *da datificação.* Inclusive, Zuboff (2020, p. 402) denomina esse poder como instrumentalismo, que busca a "instrumentação e instrumentalização do comportamento para propósitos de modificação, predição, monetização e controle" sobre as pessoas.

Sendo assim, vem à discussão a questão sobre "se" e "como" seria possível identificar algum espaço de liberdade das pessoas, que é um direito da personalidade. Foucault (1988) dedica-se então a identificar em meio às relações de poder forjadas pelos discursos, espaços de auto constituição do sujeito, espaços de exercício da liberdade Foucault, segundo explica Ruzyk (2009, p. 55), concebe que entre liberdade e poder não haveria, necessariamente, uma relação de exclusão. Em seu entender, a liberdade seria a condição de possibilidade para o poder, já que não haveria poder onde não há possibilidade de uma multiplicidade de condutas, inclusive de resistência. Não haveria verdadeiro poder onde as relações estão "saturadas", como na escravidão, por exemplo, em que, ao invés de poder, está-se diante de relação física de coação. Daí concluir Foucault que "a relação de poder e a insubmissão da liberdade não podem ser separadas" (DREYFUS; RABINOW, 1995, p. 244).

A partir desse raciocínio, a liberdade em um contexto de poder e controle, pressupõe condições de resistência. Ser livre seria resistir. É nesse viés que se considera que a liberdade, como um direito da personalidade, também apresenta conjunturas possíveis para o exercício de resistência, dentro dos limites da lei estabelecidos no Estado Democrático de Direito.

Também pode-se relacionar a política de dados com os direitos da personalidade, ao qual inclusive vincula-se da noção da liberdade e resistência, decorre da consideração das práticas de resistência como importantes e essenciais instrumentos de transformação social, na medida em que expandem as possibilidades de usuários e/ou titulares se insurgirem contra os abusos e violações perpetradas pelas *big techs*, logo, relaciona-se com a efetividade dos direitos da personalidade e a tutela da personalidade humana. Nesse viés, o ativismo de dados refere-se a táticas contra hegemônicas, defensivas que procuram alterar a relação entre os cidadãos e o *big data*, e a recolha massiva de dados, capacitando os titulares para serem mais críticos (MILAN, 2017, p. 3). Exemplificando, a desconexão pode ser entendida como uma prática de ampliação da resistência à própria conectividade e *datificação* (FIGUEIRAS; BRITES; SCHRDER, 2023, p. 179).

4 CONSIDERAÇÕES FINAIS

Esta pesquisa teve por objetivo avançar teoricamente pretender relacionar o ativismo digital com a tutela dos direitos da personalidade e da personalidade humana. Por meio do método dedutivo, buscou-se compreender a noção de ativismo de dados como uma ferramenta de tutela e proteção aos direitos da personalidade, enfatizando o ativismo de dados como uma construção teórica que se encontra em evolução.

Por meio do método de abordagem dedutivo, no primeiro item, analisou-se a ascensão da tecnologia nas formas de ativismo social. Em seguida, considerou-se esse tema no campo dos direitos da personalidade, e foi possível concluir que o ativismo digital tensiona novos contextos de disputas frente a violações aos direitos da personalidade. Além disso, fomenta a articulação de práticas individuais e coletivas que questionam o uso desses atributos da personalidade no ciberespaço.

O ativismo digital também se vincula à liberdade, a partir do raciocínio foucaultiano sobre a liberdade pressupor em seu âmbito, certas condições de resistência. Nesse viés, considera-se que a liberdade, como um direito da personalidade, também apresenta conjunturas possíveis para o exercício de resistência, dentro dos limites da lei

estabelecidos no Estado Democrático de Direito.

Por fim, também foi possível relacionar a política de dados com os direitos da personalidade, ao qual inclusive vincula-se da noção da liberdade e resistência, decorre da consideração das práticas de resistência como importantes e essenciais instrumentos de transformação social, na medida em que expandem as possibilidades de usuários e/ou titulares se insurgirem contra os abusos e violações perpetradas pelas big techs.

Ressalta-se que esta pesquisa não pretendeu esgotar a temática, mas relacionar os conceitos de ativismo digital e direitos da personalidade. Assim, visualiza-se a abertura de um novo campo de pesquisa em estudos sobre mecanismos de efetividade dos direitos da personalidade, em particular, explorando as formas de ativismo e resistência no espaço digital.

REFERÊNCIAS

ALVES, Cristiane Avancini. Os Direitos da personalidade e suas conexões intra, inter e extra-sistemáticas. **Revista jurídica:** doutrina, legislação, jurisprudência, Porto Alegre, n. 330, abr. 2005.

AMARAL, Francisco. Racionalidade e sistema do Direito civil brasileiro. **Revista de informação legislativa,** Brasília, v. 31, n. 121, p. 233-243, jan./mar. 1994. Disponível em: https://www2.senado.leg.br/bdsf/item/id/176154. Acesso em: 14 ago. 2023.

ANDRADE, Fábio Siebeneichler de. A tutela dos direitos da personalidade no direito brasileiro em perspectiva atual. **Revista de Derecho Privado**, Bogotá, n. 24, p. 81-111, jan./jul. 2013. Disponível em: https://repositorio.pucrs.br/dspace/handle/10923/11474. Acesso em: 16 ago. 2023.

ASCENSÃO, José Oliveira. Os direitos de personalidade no Código Civil Brasileiro. **Revista da Faculdade de Direito de Lisboa**, Lisboa, v. 12, p. 1-25, 2014. Disponível em: https://www.fd.ulisboa.pt/wp-content/uploads/2014/12/Ascensao-Jose-Oliveira-OS-DIREITOS-DE-PERSONALIDADE-NO-CODIGO-CIVIL-BRASILEIRO.pdf. Acesso em: 14 ago. 2023.

BAACK, Stefan. Datafication and empowerment: How the open data movement re-articulates notions of democracy, participation, and journalism. ***Big data* & Society**, v. 2, n. 2, p. 1-11, jul. 2015. Disponível em: https://doi.org/10.1177/2053951715594634. Acesso em: 25 set. 2023.

BERALDO, Davide; MILAN, Stefania. From Data Politics to the Contentious Politics of Data. ***Big data* & Society,** p. 1-11, jul./dez. 2019. Disponível em: https://ssrn.com/abstract=3487477. Acesso em: 20 set. 2023.

BITTAR, Carlos Alberto. **Os direitos da personalidade.** 8. ed. São Paulo: Saraiva, 2015.

BORGES, Roxana Cardoso Brasileiro. **Direitos da personalidade e autonomia privada.** 2. ed. São Paulo: Saraiva, 2007.

BUZANELLO, José Carlos. Em torno da Constituição do direito de resistência. **Revista de informação legislativa,** v. 42, n. 168, p. 19-27, out./dez. 2005. Disponível em: http://www2.senado.leg.br/bdsf/handle/id/917. Acesso em: 29 set. 2023.

CAMARA, Maria Amália Oliveira De Arruda. **Controle estatal da informação na internet:** Os limites definidos pelo debate democrático brasileiro entre a segurança pública e garantias individuais constitucionalmente protegidas. 2010. 130 f. Tese (Doutorado em Direito) - Universidade Federal de Pernambuco, Recife, 2010, p. 30.

CAMPOS, Ricardo; PEREIRA, Inês; SIMÕES, José Alberto. Ativismo digital em Portugal: um estudo exploratório. **Sociologia, Problemas e Práticas,** n. 82, p. 27-47, 2016. Disponível em: https://journals.openedition.org/spp/2460. Acesso em: 15 set. 2023.

CARVALHO FERNANDES, Luis. A. **Teoria Geral do Direito Civil.** vol. I. 2. ed. Lisboa: Lex, 1995.

CASTELLS, Manuel. **A Galáxia da internet:** reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Zahar, 2003.

CASTELLS, Manuel. A internet ameaçada. **Portal Fórum,** Porto Alegre, mar. 2015. Seção Outras Palavras. Disponível em: https://revistaforum.com.br/midia/2015/3/22/castells-internet-ameaada-11924.html. Acesso em: 13 jul. 2015.

CASTELLS, Manuel. **A sociedade em rede.** São Paulo: Paz e Terra, 1999.

CASTELLS, Manuel. **Networks Outrage and Hope.** Social Movements in the Internet Age, Cambridge Malden, MA: PolityPress, 2012.

CAVALCANTI, Davi Barboza; JARDELINO, Fábio; NASCIMENTO, Raíssa. Ativismo digital no Brasil contemporâneo. **Brazilian Journal of Development,** v. 6, n.

7, p. 42556-42570, 2020. Disponível em: https://ojs.brazilianjournals.com.br/ojs/index.php/BRJD/article/view/12520. Acesso em: 15 set. 2023.

COTÉ, Mark; GERBAUDO, Paolo; PYBUS, Jennifer: Introduction. Politics of *Big data*. **Digital Culture & Society,** v. 2, n. 2, p. 5-15, 2016. Disponível em: https://mediarep.org/handle/doc/3163. Acesso em: 19 set. 2023.

COULDRY, Nick; MEJIAS, Ulises A. Data colonialism: Rethinking *big data*'s relation to the contemporary subject. **Television & New Media,** v. 20, p. 1-14, 2018. Disponível em: https://doi.org/10.1177/1527476418796632. Acesso em: 24 set. 2023.

CUKIER, Kenneth; MAYER-SCHONBERGER, Viktor. ***Big data*: A Revolution That** Will Transform How We Live, Work and Think. 1. ed. London: John Murray, 2013.

DELEUZE, Gilles. Post-scriptum sobre as sociedades de controle. In: DELEUZE, Gilles. **Conversações (1972-1990).** Rio de Janeiro: Ed. 34, 1992, p. 219-226.

DESLANDES, Suely Ferreira. O ativismo digital e sua contribuição para a descentralização política. **DEBATEDORES:** Ciênc. saúde colet. ano 23, n. 10, out., p. 3133-3136, 2018. Disponível em: https://www.scielo.br/j/csc/a/qmYg4yygsjgWwmQ8MvHVM5N/. Acesso em: 15 set. 2023.

DONEDA, Danilo. PANORAMA HISTÓRICO DA PROTEÇÃO DE DADOS PESSOAIS. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR, Otávio Luiz (Coord.). **Tratado de proteção de dados pessoais.** Rio de Janeiro: Forense, 2021.

DREYFUS, Hubert L.; RABINOW, Paul. **Michel Foucault:** Uma trajetória filosófica: para além do estruturalismo e da hermenêutica. Tradução: Vera Porto Carrero. Rio de Janeiro: Forense Universitária, 1995. Disponível em: https://monoskop.org/images/2/29/Rabinow_Paul_Dreyfus_Hubert_Foucault_Uma_trajetoria_filosofica.pdf. Acesso em: 28 set. 2023.

FIGUEIRAS, Rita; BRITES, Maria José; SCHRØDER, Kim Christian. Resistência aos media e desconexão digital na literatura ocidental. **MATRIZes,** São Paulo, v. 17, n. 2, p. 171-190, 2023. Disponível em: https://www.revistas.usp.br/matrizes/article/view/201225. Acesso em: 29 set. 2023.

FONSECA, Lucas Milhomens. **Ciberativismo e MST:** o debate sobre a reforma agrária na nova esfera pública interconectada. 2009. 116 f. Dissertação (Mestrado em Comunicação) - Universidade Federal da Paraíba, João Pessoa, 2009.

FOUCAULT, Michel. **História da sexualidade:** a vontade de saber. Rio de Janeiro: Graal, 1988.

FRANÇA, Limongi. **Manual de direito civil.** 4. ed. São Paulo: Revista dos Tribunais, 1980. v. 1.

FREIRE DE SÁ, Maria de Fátima; MOUREIRA, Diogo Luna. **Autonomia para morrer:** eutanásia, suicídio assistido, diretivas antecipadas de vontade e cuidados paliativos. 2. ed. Belo Horizonte: Del Rey, 2015.

GOMES, Orlando. Direitos de personalidade. **Revista de Informação Legislativa**, v. 3, n. 11, p. 39-48, 1966. Disponível em: https://www2.senado.leg.br/bdsf/item/id/180717. Acesso em: 11 ago. 2023.

HANSEN, Derek; SHNEIDERMAN, Ben; SMITH, Marc. **Analyzing social media networks with NodeXL:** insights from a connected world. Burlington-MA: Elsevier, 2011.

HOFFMANN, Anna Lauren. Where fairness fails: data, algorithms, and the limits of antidiscrimination discourse. **Information Communication and Society,** Data Justice v. 22, n. 7, p. 900-915, 2019. Disponível em: https://doi.org/10.1080/1369118X.2019.1573912. Acesso em: 24 set. 2023.

IKEDA, Walter Lucas; TEIXEIRA, Rodrigo Valente Giublin. Direitos da Personalidade: Terminologias, Estrutura e Recepção. **Revista Jurídica Cesumar**, Maringá/PR, v. 22, n. 1, p. 129-152, jan./abr. 2022. Disponível em: https://periodicos.unicesumar.edu.br/index.php/revjuridica/article/view/10618. Acesso em: 12 ago. 2023.

JABORANDY, Clara Cardoso Machado; GOLDHAR, Tatiane Gonçalves Miranda. A repersonalização do direito civil a partir do princípio da fraternidade: um novo enfoque para tutela da personalidade na contemporaneidade. **Revista Jurídica Cesumar.** v. 18, n. 2, p. 481-502, maio/ago., 2018. Disponível em: https://periodicos.unicesumar.edu.br/index.php/revjuridica/article/view/6267. Acesso em: 12 ago. 2023.

KITCHIN, Rob. *Big data*, New Epistemologies and Paradigm Shifts. ***Big data* & Society,** v. 1, n. 1, p. 1-12, abr./jun. 2014. Disponível em: https://doi.org/10.1177/2053951714528481. Acesso em: 20 set. 2023.

LEMOS, André. Nova esfera conversacional. In DIMAS, A. et al. **Esfera pública, redes e jornalismo.** Rio de Janeiro: Ed. E-Papers, 2009. p. 9-30.

LIMA, Gabriela Bezerra. Tipos de Ativismo Digital e Ativismo Preguiçoso no Mapa Cultural. **Revista GEMInIS**, ano 3, n. 1, p. 71-96, 2012. Disponível em: https://www.revistageminis.ufscar.br/index.php/geminis/article/download/99/73/308. Acesso em: 15 set. 2023.

MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. ***Big data*****:** a revolution that will transform how we live, work and think. London: John Murray. 2013.

MEDEIROS, Priscila Muniz de; LORDÊLO, Tenaflae da Silva. Ciberativismo e a influência da opinião pública sobre a esfera privada: os protestos contra o uso de peles na indústria da moda. **Revista GEMInIS,** v. 3, n. 1, p. 110–124, 2012. Disponível em: https://www.revistageminis.ufscar.br/index.php/geminis/article/view/101. Acesso em: 15 set. 2023.

MEJIAS, Ulises A.; COULDRY, Nick. Datafication. **Internet Policy Review,** v. 8, n. 4, 2019. Disponível em: https://doi.org/10.14763/2019.4.1428. Acesso em: 24 set. 2023.

MENDES, Laura Schertel Ferreira. **Transparência e privacidade:** violação e proteção da informação pessoal na sociedade de consumo. 2008. 158 f. Dissertação (Mestrado em Direito) - Universidade De Brasília, Brasília, 2008.

MILAN, Stefania. Data Activism as the New Frontier of Media Activism In: **Media Activism in the Digital Age.** New York: Routledge, 2017. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2882030. Acesso em: 28 set. 2023.

MILAN, Stefania. Hacktivism as a Radical Media Practice. In: **Routledge Companion to Alternative and Community Media.** New York: Routledge, 2015, p. 550-560.
MILAN, Stefania. When Algorithms Shape Collective Action: Social Media and the Dynamics of Cloud Protesting. **Social Media + Society,** v. 1, n. 2, p. 1-10, jul/dez, 2015. Disponível em: https://doi.org/10.1177/2056305115622481. Acesso em: 20 set. 2023.

MILAN, Stefania; GUTIÉRREZ, Miren. Citizens' media meets *big data*: the emergence of data activism. **Mediaciones,** v. 11, n. 14, p. 120-133, fev. 2015. Disponível em: https://doi.org/10.26620/uniminuto.mediaciones.11.14.2015.120-133. Acesso em: 24 set. 2023.

MILAN, Stefania; VAN DER VELDEN, Lonneke. The Alternative Epistemologies of Data Activism. **Digital Culture & Society,** Politics of *Big data*, v. 2. n. 2, p. 57-74, 2016. Disponível em: https://mediarep.org/handle/doc/3166. Acesso em: 20 set. 2023.

MIRANDA, Pontes. **Tratado de Direito Privado:** parte especial. Tomo VII: Direito de personalidade. Direito de família: direito matrimonial. 1. ed. Atualizado por Rosa Maria de Andrade Nery. São Paulo: Revista dos Tribunais, 2012.

MOREIRA, Mayume Caires. **O acesso às tecnologias de informação e comunicação no Brasil:** uma análise crítica da exclusão e da desigualdade digital sob a perspectiva dos direitos da personalidade. 2022. 193 f. Dissertação (Mestrado em Ciências Jurídicas) - Programa de Pós-Graduação em Ciências Jurídicas, Universidade Cesumar, Maringá, 2022.

MOSTAFA, Solange Puntel; CRUZ, Denise Viuniski da Nova; AMORIM, Igor Soares. Primavera nos dentes: fuga e resistência na era digital | Spring in your teeth: escape and resistance in the digital era. **Liinc em Revista,** Rio de Janeiro, RJ, v. 11, n. 2, p. p. 360-374, nov. 2015. Disponível em: https://revista.ibict.br/liinc/article/view/3665. Acesso em: 29 set. 2023.

PERLINGIERI, Pietro. **Perfis do direito civil.** Rio de Janeiro: Renovar, 1999.

RAMINELLI, Francieli Puntel; FELTRIN, Lohana Pinheiro; OLIVEIRA, Rafael Santos de; CHRISTO, Tatiana Vielmo de. **Ciberativismo do consumidor 2.0:** limites e oportunidades ao exercício do direito de expressão no ciberespaço. Disponível em: https://egov.ufsc.br/portal/conteudo/ciberativismo-do-consumidor-20-limites-e-oportunidades-ao-exerc%C3%ADcio-do-direito-de-express%C3%A3o. Acesso em: 29 set. 2023.

REIS, Patrícia dos; OLIVEIRA, Rafael Santos de. A atuação dos movimentos sociais por meio do ciberativismo na defesa dos direitos dos infantes: uma análise do projeto criança e consumo e suas ações no combate à publicidade infantil. **Rev. de Movimentos Sociais e Conflitos,** Maranhão, v. 3, n. 2, p. 38-57, jul/dez, 2017. Disponível em: https://www.indexlaw.org/index.php/revistamovimentosociais/article/view/2524. Acesso em: 15 set. 2023.

RODRIGUEZ, Igor Sádaba; ROIG, Gustavo Roig. Nodo 50: territorio virtual para los movimientos sociales y la acción política. In: SÁEZ, Víctor Manuel Marí. **La red es de todos:** cuando los movimientos sociales se apropian de la red, 2004, p. 195-234 Disponível em: https://dialnet.unirioja.es/servlet/articulo?codigo=885615. Acesso em: 25 set. 2023.

RUPPERT, Evelyn; ISIN, Engin Isin; BIGO, Didier. Data politics. ***Big data* & Society,** v. 4, n. 2, p. 1-7, jul./dez. 2017. Disponível em: https://doi.org/10.1177/2053951717717749. Acesso em: 21 set. 2023.

RUZIK, Carlos Eduardo Pianovski. **Liberdade(s) e função:** contribuição crítica para uma nova fundamentação da dimensão funcional do Direito Civil brasileiro. 2009. 402 f. Tese (Doutorado em Direito) - Programa de Pós-Graduação em Direito da Universidade Federal do Paraná, 2009.

SALDANHA, Rodrigo Róger; OLIVEIRA, José Sebastião de. A quarta expressão dos direitos da personalidade: o conjunto informativo digital como um novo conceito no Direito Civil contemporâneo. **Revista Húmus,** [S. l.], v. 12, n. 37, 2022. Disponível em: https://periodicoseletronicos.ufma.br/index.php/revistahumus/article/view/19182. Acesso em: 29 set. 2023.

SANTOS, Fernando. **O ciberativismo como ferramentas de grandes mobilizações humanas:** das revoltas no Oriente Médio às ações pacíficas do Greenpeace no Brasil. São Paulo: Anagrama, 2011.

SIQUEIRA, Dirceu Pereira; MOREIRA, Mayume Caires; VIEIRA, Ana Elisa Silva Fernandes. As pessoas e grupos em exclusão digital: os prejuízos ao livre desenvolvimento da personalidade e a tutela dos direitos da personalidade. **Revista Direitos Culturais,** Santo Ângelo, v. 18, n. 45, p. 3-17, maio/ago. 2023. Disponível em: https://san.uri.br/revistas/index.php/direitosculturais/article/view/1129. Acesso em: 20 set. 2023.

SOARES, Ana Thereza Nogueira. Epistemologia, métodos e teorias da comunicação na era do *Big data*: panorama crítico da pesquisa em mídias sociais. **Comunicação e Sociedade,** Braga, Portugal, v. 33, p. 151-166, 2018. Disponível em: https://revistacomsoc.pt/index.php/revistacomsoc/article/view/1059. Acesso em: 19 set. 2023.

SZANIAWSKI, Elimar. **Direitos de personalidade e sua tutela.** 2. ed. São Paulo: Revista dos Tribunais, 2005.

TEPEDINO, Gustavo. **Fundamentos do direito civil:** teoria geral do direito civil. E-book. 3. ed. Rio de Janeiro: Forense, 2022.

TEPEDINO, Gustavo. **Temas de direito civil.** 3.ed. Rio de Janeiro: Renovar, 2004.

TUFEKCI, Zeynep. Engineering the public: *Big data*, surveillance and computational politics. **First Monday,** [S. l.], v. 19, n. 7, 2014. Disponível em: https://firstmonday.org/ojs/index.php/fm/article/view/4901. Acesso em: 25 set. 2023.

VASCONCELOS FILHO, José Marques de; COUTINHO, Sérgio. **O ativismo digital brasileiro.** São Paulo: Fundação Perseu Abramo, 2016.

VEGH, S. **Classifying forms of online activism:** the case of cyberprotests against the World Bank. In: MCCAUGHEY, M., AYERS, M.D. (org.). Cyberactivism: online activism in theory and practice. London: Routledge, 2003.

WACKS, Raymond. **Personal Information:** Privacy and the Law. Oxford, Clarendon Press, 1989.

ZANINI, Leonardo Estevam de Assis; QUEIROZ, Odete Novais Carneiro. A inviolabilidade da pessoa humana e o direito geral da personalidade. **Revista Brasileira de Direito Civil,** Rio de Janeiro, v. 27, n. 01, p. 15, 2021. Disponível em: https://rbdcivil.emnuvens.com.br/rbdc/article/view/535. Acesso em: 29 set. 2023.

ZUBOFF, Shoshana. **A Era do Capitalismo de Vigilância:** A luta por um futuro humano na nova fronteira do poder. Tradução: George Schlesinger. Rio de Janeiro: Intrínseca, 2020.

A UTILIZAÇÃO DO PROCESSO JUDICIAL ELETRÔNICO PELO PODER JUDICIÁRIO E ADOÇÃO DE NOVAS TECNOLOGIAS COMO FORMA DE DEMOCRATIZAÇÃO DO ACESSO À JUSTIÇA

THE USE OF THE ELECTRONIC JUDICIAL PROCESS BY THE JUDICIARY AND ADOPTION OF NEW TECHNOLOGIES AS A WAY OF DEMOCRATIZING ACCESS TO JUSTICE

Altair Resende de Alvarenga[1]

Resumo: O presente artigo tem por objetivo analisar a transição dos conflitos levados à justiça, que eram realizados através de protocolização em meio físico e atualmente realiza-se através da utilização do Processo Judicial Eletrônico-PJe. Para tanto, será feita a apresentação da forma e quais são os meios de acesso ao sistema eletrônico, trazendo definições dos princípios com maior destaque sobre o tema. Ocorrerá o levantamento dos principais aspectos da Lei do Processo Eletrônico, destacando os pontos relevantes e os que impulsionam o andamento processual. O estudo também irá analisar as ferramentas digitais utilizadas pelos órgãos públicos e evidenciar que a utilização da tecnologia pode servir como forma para alcance de maior acesso à justiça pelos jurisdicionados, eliminando barreiras físicas, temporais e econômicas, contribuindo assim para uma justiça mais célere, eficiente e transparente.

Palavras-chave: Acesso à Justiça; Poder Judiciário; Processo Judicial Eletrônico.

Abstract: This article aims to analyze the transition of conflicts brought to justice, which were carried out through physical protocolization and are currently carried out through the use of the Electronic Judicial Process-PJe. To this end, the form and means of access to the electronic system will be presented, providing definitions of the most prominent principles on the topic. The main aspects of the Electronic Process Law will be surveyed,

[1] Doutor em Ciências Jurídicas e Sociais pela Universidad deo Museo Social Argentino - UMSA, título apostilado e reconhecido no Brasil pela Universidade Federal de Campina Grande. Mestrando em Direito nas Relações Econômicas e Sociais pela Faculdade Milton Campos. Pós-graduado em Direito Público pela Faculdade Integradas do Oeste de Minas (FADOM). Pós-graduado em Direito Civil pela Pontifícia Universidade Católica de Minas Gerais (PUC/MG). Juiz de Direito nas Comarcas de Formiga/MG e Itapecerica/MG. Professor titular do Centro Universitário de Formiga das disciplinas de Direito Penal, Família, Prática Jurídica e Direito Processual Penal I. Lattes: http://lattes.cnpq.br/8401214885708451.

highlighting the relevant points and those that drive the procedural progress. The study will also analyze the digital tools used by public bodies and highlight that the use of technology can serve as a way to achieve greater access to justice for those under jurisdiction, eliminating physical, temporal and economic barriers, thus contributing to faster, more efficient justice and transparent.

Keywords: Access to Justice; Judicial power; Electronic Judicial Process.

1 INTRODUÇÃO

O Poder Judiciário precisou se reinventar estruturalmente durante o período em que o mundo vivenciou a pandemia provocada pelo coronavírus, com início em 2019, atualmente superada graças às políticas governamentais de vacinação implementadas. No entanto, diversos foram os aprendizados tecnológicos extraídos durante o período para utilização futura no âmbito dos poderes públicos, especialmente pelo Poder Judiciário, tendo em vista que, para ultrapassar todas as barreiras impostas pelas medidas sanitárias, visando a continuidade da prestação jurisdicional e do acesso à justiça pelos cidadãos, a adaptação tecnológica se fez necessária aos processos judiciais.

Imprescindivelmente, essas transformações modificaram subitamente o procedimento de instrução no processo civil, tornando cada vez mais comum a substituição dos ritos presenciais pelas modalidades de videoconferência ou de atos realizados por meio eletrônico.

Dessa forma, o presente artigo destacará as inovações tecnológicas implementadas pelo Poder Judiciário e demonstrará que sua utilização pode incrementar o acesso à justiça, eliminando as barreiras físicas, econômicas e temporais outrora existentes, eis que a utilização da tecnologia da informação no processo judicial trouxe grandes benefícios à tramitação processual no que diz respeito ao acesso ao judiciário.

A primeira parte do artigo versará sobre o acesso à justiça: princípio constitucional e compromisso com os jurisdicionados e uma análise à luz dos demais princípios constitucionais processuais. Na sequência, a segunda parte discorrerá sobre o processo judicial eletrônico: mudanças e impactos na proteção de direitos fundamentais.

Por fim, a terceira parte do trabalho pontuará algumas inovações tecnológicas implementadas pelo Poder Judiciário, bem como irá ponderar os consequentes reflexos práticos e jurídicos, com análise de aspectos positivos e negativos dos meios tecnológicos e digitais implantados pelos órgãos públicos nacionais.

2 ACESSO À JUSTIÇA: PRINCÍPIO CONSTITUCIONAL E COMPROMISSO COM OS JURISDICIONADOS

O acesso à justiça não se trata apenas do simples ingresso ao juízo, mas sim do oferecimento da grande admissão de causas e pessoas ao processo, garantindo-lhes a observância das regras que fortalecem o processo legal e a participação na formação do convencimento do juiz, criando uma solução justa que exclua os resíduos de insatisfação ou sentimento de injustiça.

A Constituição da República Federativa do Brasil de 1988 tem por objetivo conservar conquistas acrescentadas ao patrimônio da humanidade e avançar na direção de valores e bens jurídicos desejáveis e ainda não alcançados, sendo o processo judicial várias vezes a única forma de se fazer com que os valores incorporados sejam cumpridos, alcançando assim o fim a que se pretende. (DELGADO, 1997).

Os princípios são normas que ordenam que algo seja realizado dentro das possibilidades jurídicas e fáticas existentes; em relação ao acesso à justiça, procura-se a mais ampla discussão de causas e pessoas ao processo para uma solução justa. Nesse viés, no que diz respeito ao acesso à justiça, existe uma preocupação em melhorar e modernizar os procedimentos, em torná-los mais céleres, investir em decisões mais compreensíveis pelas partes, redução de custos e a tentativa de que as partes fiquem em pé de igualdade. (CAPPELLETTI, 1988).

O princípio do acesso à justiça ou acesso à ordem jurídica justa, desata a ideia salientada no inciso XXXV do artigo 5º da Constituição da República Federativa do Brasil de 1988: "A lei não excluirá da apreciação do Poder Judiciário lesão ou ameaça a direito". (BRASIL, 1988).

Foi na década de 1980 que o movimento de renovação de acesso à justiça ganhou força com o "Projeto Florença" ou Movimento de Acesso à Justiça, realizado por Mauro Cappelletti e Bryant Garth, onde foram propostas ondas renováveis de acesso à justiça que tinham a finalidade de analisar as ferramentas de acesso, de modo que tornassem efetivo e transpusessem as barreiras nos sistemas judiciais para a sua concretização. (PASCHOAL, 2021).

Na primeira onda renovatória reconheceu-se o problema da desigualdade quanto ao acesso, que limitava a participação apenas aos indivíduos economicamente privilegiados, surgindo assim a defesa pela assistência jurídica gratuita. Na segunda onda, observou-se que tradicionalmente o processo era focado no individualismo, defendendo assim a existência de um procedimento adequado quando os demandantes formam uma massa desfavorecida. Na terceira onda, verificou-se a necessidade de meios pacíficos na resolução de conflitos, buscando soluções consensuais e alternativas ao litígio judicial, viabilizando métodos como a mediação com soluções mais rápidas. (CAPPELLETTI; GARTH, 1988).

O acesso à justiça surge com a procura da resolução instrumental pelo Poder Judiciário, indo além da procura pelas portas da justiça, envolvendo também a busca pelo acesso digno, humanizado e principalmente efetivo à justiça, garantindo dessa forma uma tutela jurisdicional efetiva e promovendo a realização dos valores públicos.

Em relação à tutela jurisdicional efetiva, os autores Marinoni, Arenhart e Mitidiero (2017, p. 521) destacam que: “o exercício da Jurisdição será legítimo quando respeitar o direito à adequada participação, garantir o uso da técnica adequada à tutela do direito material e resultar em uma decisão que respeite os direitos fundamentais”.

A linguagem “acesso à justiça” representa a possibilidade de alcançar algo, que é o valor "justiça", pois é um mandamento fundamental que informa todo o ordenamento jurídico. O novo Código de Processo Civil de 2015 usa o termo "Acesso à Justiça" ao

tratar da cooperação jurídica internacional e da petição inicial, previstas no art. 26[2], inc. II e art. 319[3], §3º do diploma normativo processual.

O alcance de acesso à justiça deve ser mais amplo do que simplesmente o acesso ao Poder Judiciário, isto é, o direito e a garantia do acesso à justiça não se esgotam com a simples entrega da prestação jurisdicional, sem a preocupação da realização da ordem jurídica justa. Segundo menciona a autora Grinover (1994, p. 07): "é necessário, ainda, contar, quando possível, com a participação popular, no que é chamado, atualmente, de "quadro da democracia participativa", ante o alargamento da legitimidade *ad causam*, como ocorre nos casos das ações coletivas".

O acesso à justiça significa proporcionar a todos, sem restrições, o direito de pleitear a tutela jurisdicional do Estado. Ninguém pode ser privado do devido processo constitucional em conformidade com as garantias fundamentais, que o tornam correto, logo, só pode falar-se em princípio do acesso à justiça quando do acesso a ordem jurídica justa.

2.1 Uma análise à luz dos demais princípios constitucionais processuais

O princípio constitucional do devido processo legal traduz que todo sujeito de direito possui direito fundamental a um processo justo e equitativo, apresentando uma

[2] Art. 26. A cooperação jurídica internacional será regida por tratado de que o Brasil faz parte e observará: (...) II – a igualdade de tratamento entre nacionais e estrangeiros, residentes ou não no Brasil, em relação ao acesso à justiça e à tramitação dos processos, assegurando-se assistência judiciária aos necessitados (...). (BRASIL, 2015).

[3] Art. 319. A petição inicial indicará: I – o juízo a que é dirigida; II – os nomes, os prenomes, o estado civil, a existência de união estável, a profissão, o número de inscrição no Cadastro de Pessoas Físicas ou no Cadastro Nacional da Pessoa Jurídica, o endereço eletrônico, o domicílio e a residência do autor e do réu; III – o fato e os fundamentos jurídicos do pedido; IV – o pedido com as suas especificações; V – o valor da causa; VI – as provas com que o autor pretende demonstrar a verdade dos fatos alegados; VII – a opção do autor pela realização ou não de audiência de conciliação ou de mediação. § 1°. Caso não disponha das informações previstas no inciso II, poderá o autor, na petição inicial, requerer ao juiz diligências necessárias a sua obtenção. § 2°. A petição inicial não será indeferida se, a despeito da falta de informações a que se refere o inciso II, for possível a citação do réu. § 3°. A petição inicial não será indeferida pelo não atendimento ao disposto no inciso II deste artigo se a obtenção de tais informações tornar impossível ou excessivamente oneroso o acesso à justiça. (BRASIL, 2015).

garantia contra o exercício abusivo do poder. Deste princípio decorrem pressupostos básicos como o julgamento por juiz natural, o contraditório e ampla defesa e a necessidade de um procedimento célere e eficiente. (MIRANDA DE OLIVEIRA, 2017).

O princípio do devido processo legal deve ser empregado de maneira a cumprir constitucionalmente o estabelecido e garantir o total acesso à justiça pela possibilidade de o indivíduo levar sua pretensão de direito ao Judiciário e proporcionar a observância das normas processuais previstas no desenrolar do processo.

Por sua vez, o princípio da isonomia determina que o juiz deverá dirigir o processo assegurando às partes uma igualdade de tratamento, que não seja simplesmente formal, mas que obedeça a regra de uma paridade mais efetiva, assegurando, assim, o tratamento equilibrado. Nesse sentido, o autor Nery Júnior (2000, p. 43) ressalta que: "para garantia da isonomia, sob o prisma do acesso à justiça, deve-se tratar igualmente os iguais e desigualmente os desiguais, na exata medida de sua desigualdade".

Enfatiza o autor Didier Jr. (2020, p. 110) que a igualdade processual deve observar quatro aspectos principais: "a imparcialidade do juiz pela equidistância em relação as partes, a ausência de discriminação, a redução das desigualdades que dificultem o acesso à justiça como a financeira e a igualdade no acesso às informações necessárias ao contraditório".

A seu turno, o princípio do contraditório certifica o princípio da igualdade, visto que garante o mesmo tratamento efetivo no processo para a elaboração da decisão final. A ampla defesa é um interesse público que compreende o conjunto de meios convenientes para o exercício do adequado contraditório, sendo que ambos formam um par de garantias previstas na Constituição da República Federativa do Brasil de 1988.

O princípio do juiz natural, previsto na Constituição da República Federativa do Brasil de 1988, relaciona-se à existência de juízo adequado para o julgamento de certa demanda, de acordo com as regras de fixação de competência, e a proibição de juízos extraordinários ou tribunais de exceção constituídos após os fatos. Conforme realça Barroso (1998, p. 35):

> O postulado do juiz natural, por encerrar uma expressiva garantia da ordem constitucional, limita, de modo subordinante, os poderes do Estado — que fica, assim, impossibilitado de instituir juízos ad hoc ou de criar tribunais de exceção —, ao mesmo tempo em que assegura ao acusado o direito ao processo perante autoridade competente abstratamente designada na forma da lei anterior, vedados em consequência, os juízos *ex post facto.*

O direito à inafastabilidade do controle jurisdicional tem previsão na Constituição da República Federativa do Brasil de 1988, em seu art. 5º, inc. XXXV, que dispõe: "a lei não excluirá da apreciação do Poder Judiciário lesão ou ameaça a direito". Este princípio aponta o monopólio estatal na distribuição da justiça, quanto ao amplo acesso de todos os cidadãos.

Lado outro, o princípio da publicidade consiste em uma garantia ao jurisdicionado sobre a possibilidade de controle da atuação do Poder Judiciário frente às demandas apresentadas, proporcionando a fiscalização e o acompanhamento em tempo real do processo e seus desdobramentos.

Essa regra de publicidade, conforme versada na Constituição da República Federativa do Brasil de 1988, só encontra exceção em defesa da intimidade e interesse social, sendo priorizada a publicidade restrita, para que não seja violado o direito à privacidade, zelando assim pela segurança de dados sensíveis pessoais.

O princípio da efetividade garante que os direitos devem não ser apenas reconhecidos, mas também efetivados. A efetividade na jurisdição permite o alcance da finalidade do processo, proporcionando ao jurisdicionado a tutela jurisdicional mais correta e satisfatória. Sobre o princípio da efetividade, o autor Didier Júnior (2020, p. 110) evidencia que:

> Esse princípio está intrinsicamente relacionado com a gestão do processo e o órgão jurisdicional, no trâmite processual, deve ser visto como administrador, que deve aplicar os poderes de condução conferidos pelas leis processuais para dar o máximo de eficiência ao processo, sendo indispensável o diálogo entre a ciência processual e do direito administrativo.

Por sua vez, o princípio da motivação das decisões judiciais é tido como garantia das partes com vistas à possibilidade de certa impugnação, com objetivo de conferir a

imparcialidade do juiz, a legalidade e a justiça das decisões. (MIRANDA DE OLIVEIRA, 2017).

Tal princípio traduz que as decisões devem ser fundamentadas, sob pena de nulidade. Ao acesso à justiça, deve ser instigado a qualidade e coerência das decisões judiciais, com decisões compreensíveis e bem fundamentadas, visto que a qualidade das decisões judiciais é diretamente proporcional à satisfação dos jurisdicionados com a prestação da tutela pretendida pelo Poder Judiciário.

3 PROCESSO JUDICIAL ELETRÔNICO: MUDANÇAS E IMPACTOS NA PROTEÇÃO DE DIREITOS FUNDAMENTAIS

O Processo Judicial Eletrônico - PJe foi criado para acabar com a tramitação de autos em papel no Poder Judiciário, permitindo que magistrados, servidores e advogados pratiquem atos processuais diretamente no sistema, além de garantir a confiabilidade do processo judicial através do uso da certificação digital.

A finalidade principal do PJe é formar e manter um sistema de processo judicial eletrônico capaz de permitir a prática de atos processuais pelos magistrados, servidores e demais participantes da relação processual diretamente no sistema, bem como o acompanhamento desse processo judicial.

O autor Feóla (2014, p. 20), sobre o tema, aduz que: “o processo judicial eletrônico situa-se neste campo da ciência. É uma forma, um instrumento de realização de atos processuais cuja finalidade é a composição do litígio e pacificação social mediante o uso da ferramenta eletrônico”.

A primeira versão do PJe foi firmada em abril de 2010, no Tribunal Regional Federal da 5ª Região, sediado no Recife. A partir daí, sua utilização foi expandida para outros tribunais, cortes estaduais, todos os Tribunais Regionais do Trabalho e para o Tribunal Superior Eleitoral. (TRF-5, 2023).

Em 2006, a promulgação da Lei n.º 11.419 forneceu base para uma revolução no processo civil, pois esta lei regulamenta o procedimento na tramitação do processo

eletrônico, além de alterar alguns dispositivos no Código de Processo Civil, normatizando alguns atos processuais. O autor Calmon (2008, p. 49) aduz que:

> A Lei nº 11.419, em seus 22 artigos, é organizada em quatro capítulos. O capítulo primeiro trata da informatização do processo judicial, onde são estabelecidas as regras básicas para a criação de um sistema de comunicação eletrônica. O segundo capítulo trata especificamente da comunicação eletrônica dos atos processuais. Iniciando se formalmente no art. 4º, observa-se que desde o terceiro artigo a nova lei já trata da Comunicação dos atos processuais. O capítulo três trata do processo eletrônico, prevendo-se o processo sem papel, com autos digitais. O capítulo quatro, sob a denominação "disposições gerais e finais", trata, ainda da informatização do processo judicial, mas é nessa parte (art. 20) que se encontram as alterações procedidas no código de Processo Civil.

A partir daí, além dos processos nos Juizados Especiais Federais, os processos comuns ordinários também tinham lei dispondo sobre a tramitação exclusivamente eletrônica, com a substituição total, ou quase total do papel por mídia eletrônica, conforme expõe Abrão (2011, p. 08):

> Ao delinear a Lei 11.419/2006 em 22 artigos, buscou o legislador objetividade, consistência e, acima de tudo, transparência na precisão do informe catalogado no diploma normativo. Não se cogita mais, felizmente, do processo papel e das incontáveis filas que aguardam distribuição e remessa aos setores de julgamento, além do difícil manuseio e custos elevados. A principal virtude do processo eletrônico é de permitir não apenas o acompanhamento de etapas e fases procedimentais, mas sobretudo, priorizar velocidade compatível com a natureza do litígio. Referida estrutura peca por algumas falhas, mas, no mesmo tempo, consegue reunir maiores vantagens e trabalhar, plenamente, suficiente banco de dados que armazena o histórico do processo. Concretamente, os elementos do processo por meio eletrônico transmitem, desde a inicial até a decisão final com trânsito em julgado, uma série de etapas e procedimentos, livres de papel, ou de volumes, o que é essencial para o reconhecimento da credibilidade de um Judiciário de amplo acesso democrático. Nessa linha de pensamento, numa primeira etapa, o legislador cuidou da informatização do processo judicial, preceito que se aplica indistintamente aos feitos civis, penais e trabalhistas, espalhando seus efeitos para os Juizados Especiais. Bem importante destacar que todos os Judiciários do país estão sob a disciplina do processo eletrônico, cada um com determinada especificidade e curial instrumento, diante do aspecto processual inerente.

A partir do ano de 2010, todos os processos da Justiça Federal passariam a tramitar de forma virtual, devido a evolução alavancada do processo eletrônico pela Lei n.º 11.416/06 e pela meta 10 do CNJ, conforme apresenta o autor Leal Júnior (2010, p. 01):

> A informatização da justiça e a implantação do processo eletrônico são passos definitivos para substituição do processo-papel pelo processo digital. A Lei 11.419, de 2006, abriu caminho para adoção do processo eletrônico. A meta 10 do CNJ de 2009 previu a implantação do processo eletrônico em parcela das unidades judiciárias dos tribunais. E a partir do início de 2010 todos os novos processos da Justiça Federal tramitarão exclusivamente no meio eletrônico. Em termos de Justiça Federal, as mudanças serão revolucionárias. A extinção do papel terá repercussões não apenas na tramitação dos processos, mas também na forma como serão praticados os atos processuais e produzidos os textos de petições e decisões.

O PJe centraliza todo o trâmite processual do Judiciário brasileiro em um único sistema através de qualquer computador conectado à internet, estando assim em constante melhoria. Dentre as várias vantagens do PJe, destaca-se a disponibilidade, a celeridade, a integridade, a sustentabilidade, a resiliência e a acessibilidade.

Nesse contexto, o PJe é virtualmente acessível 24 horas por dia, logo, a disponibilidade contínua do PJe tem viabilizado magistrados a despacharem demandas urgentes mesmo fora do expediente. Desse modo, o PJe evita o deslocamento a vários cartórios e o desperdício de papel e dinheiro com inúmeras cópias dos processos.

O PJe é um conjunto de arquivos organizados através de uma plataforma eletrônica, com o objetivo de manter a guarda dos documentos, em demandas eletrônicas, com juntadas de documentos novos, pelas partes, ativa e passiva, ou outros operadores. Assim, o processo pode ser acessado através da internet em qualquer parte do mundo.

A celeridade é uma grande vantagem, não só do PJe, mas de todos os processos eletrônicos em geral. Com o avanço das tecnologias de informação e comunicação, a própria sociedade exige que o Estado entre totalmente na era da informatização, eliminando assim trâmites burocráticos, filas e deslocamentos físicos.

No campo do direito processual civil, por exemplo, um sistema de processo eletrônico pode proporcionar ganhos de tempo ao eliminar as juntadas manuais, ao

disponibilizar os despachos, decisões e sentenças para consulta pública após assinados eletronicamente pelo juiz, quando quase todos os expedientes como alvarás, mandados, cartas, dentre outros podem ser redigidos automaticamente pelo sistema e quando os prazos processuais podem ser contados pelo próprio sistema, diminuindo assim as chances de erro e prejuízos às partes.

Sobre a celeridade processual, o autor Filho (2015, p. 206) aponta que:

> Apenas com a implantação do PJE, ocorre um ganho imediato na celeridade processual pela supressão de ocasiões em que o processo dependeria de intervenção humana para seu prosseguimento: entre o decurso do prazo e a conclusão, entre o despacho e sua publicação, entre a protocolização e a juntada da petição. Todas estas atividades são assumidas pelo sistema. Este talvez seja o ponto crucial do processo eletrônico: juízes e serventuários podem ter menos preocupações procedimentais, e concentrar-se mais nas atividades intelectuais.

Em relação à integridade, o processo eletrônico não pode ser facilmente adulterado por aqueles que manuseiam. Os autos poderiam ser modificados sem deixar vestígios, apenas com uma invasão aos bancos de dados que sustentam o processo eletrônico, o que é considerado mais complexo do que falsificar documentos em papel.

Não existem sistemas totalmente imunes a ataques, logo, políticas de segurança da informação adequadas são fundamentais para garantirem a legitimidade dos autos digitais, pois quando implementadas corretamente reduzem as chances de invasão a quase zero.

Quanto à sustentabilidade, o PJe, por ser virtual, dispensa o papel, a tinta, e os deslocamentos de partes, magistrados e auxiliares. É nítido o benefício ao meio ambiente devido a extinção dos autos físicos em todo os órgãos do Judiciário. O fim do uso do papel relaciona-se à preservação de áreas de florestas e a desnecessidade de locomoção se adequa a tempos de tráfego saturado e produção energética em crise.

Um grande destaque também para a sustentabilidade do PJe refere-se à desocupação física dos cartórios e dos escritórios, que não mais precisarão de espaços reservados para armazenamento. Muitas varas e gabinetes já são compostas apenas de

servidores e juízes, cada um com seu computador, sem a presença de estantes e armários repletos de processos.

A tecnologia permite alta disponibilidade e resiliência a custos mais baixos. A resiliência organizacional significa a capacidade de resistência às adversidades e reação diante de uma nova situação. Os autos eletrônicos são impossíveis de serem destruídos, exceto em caso de catástrofe de proporções nacionais ou de enorme negligência humana. As atuais tecnologias de *backup* em nuvem não permitem a perda e extravio dos autos.

Em relação à acessibilidade, tendo em vista que ainda não são todos os Fóruns nacionais que são adaptados a cadeirantes, o PJe é de grande ajuda por dispensar as idas e vindas às varas. Quanto ao deficiente visual, o PJe possui aplicativo de texto para fala, retirando a necessidade de participação de terceiros.

Com a implantação do sistema eletrônico, o andamento do processo tem condições de tramitar de maneira mais rápida em comparação aos feitos físicos, conforme apresenta o autor Abrão (2011, p. 09) em suas considerações:

> A principal virtude do processo eletrônico é de permitir não apenas o acompanhamento de etapas e fases procedimentais, mas, sobretudo, priorizar velocidade compatível com a natureza do litígio. Referida estrutura peca por algumas falhas, mas, ao mesmo tempo consegue reunir maiores vantagens e trabalhar, plenamente, suficiente banco de dados que armazena o histórico do processo. Concretamente, os elementos do processo por meio eletrônico transmitem, desde a inicial até a decisão final com trânsito em julgado, uma série de etapas e procedimentos, livres de papel, ou de volumes, o que é essencial para o reconhecimento da credibilidade de um Judiciário de amplo acesso democrático. Nessa linha de pensamento, numa primeira etapa, o legislador cuidou da informatização do processo judicial, preceito que se aplica indistintamente aos feitos cíveis, penais e trabalhistas, espalhando seus efeitos para os Juizados especiais. Bem importante destacar que todos os Judiciários do país estão sob a disciplina do processo eletrônico, cada um com determinada especificidade e curial instrumento, diante do aspecto processual inerente.

Com o processo eletrônico, intimam-se simultaneamente as partes com apenas um clique, podendo os processos serem acompanhados de qualquer lugar, como declara Silva Lopes (2007, p. 55):

> (...) dentre os vários benefícios, está a mobilidade. Os novos conceitos de TI (Tecnologia da Informação) convergem para a descentralização de pontos ou estações de trabalho (workstation), de forma que os profissionais possam interagir com suas atividades de qualquer lugar do globo. Aliás, com a atividade jurídica não é diferente. O operador do direito poderá, por exemplo, peticionar eletronicamente, analisar os autos via internet, apor assinaturas digitais, enfim, acompanhar processos em qualquer lugar do país, estando, inclusive, em qualquer lugar do mundo.

Maior celeridade e possibilidade de um amplo acesso ao Judiciário, um dos objetivos almejados no "novo" Código de Processo Civil, com a difusão do processo eletrônico para todos os processos e pela possibilidade de agilidade que o procedimento processual eletrônico possibilita, a tramitação judicial eletrônica, certamente, é um caminho sem volta.

4 INOVAÇÕES TECNOLÓGICAS IMPLEMENTADAS PELO PODER JUDICIÁRIO: REFLEXOS PRÁTICOS E JURÍDICOS

O Poder Judiciário, com o intuito de superar os impactos pandêmicos ocasionados outrora pelo coronavírus, ajustou suas práticas processuais para prosseguir com as atividades judiciais, como, por exemplo, com a realização de audiências por videoconferência, a fim de evitar o contato físico e respectivo contágio pelo vírus no momento em que o país vivenciava a pandemia Covid-19, atualmente superada.

Em julho de 2020, o Conselho Nacional de Justiça estabeleceu os critérios para a realização de audiências e outros atos processuais por videoconferência, principalmente para processos penais e de execução penal, de acordo com a Resolução n.º 329, determinando que sejam observados os princípios constitucionais próprios ao devido processo legal e a garantia do direito das partes.

No momento crucial da pandemia no país, foi através de expedientes virtuais que os tribunais se mantiveram atuantes, sendo que os servidores trabalhavam de maneira remota. Porém, a pandemia não gerou somente efeitos passageiros na prática jurisdicional. Embora as atividades dentro dos tribunais atualmente já retornaram, e as

audiências voltaram a ocorrer de forma presencial, verifica-se a existência de novas políticas judiciais herdadas do período pandêmico, que passaram a ser adotadas também no pós-pandemia.

O Conselho Nacional de Justiça, através da publicação "Justiça em Números-2022", indicou quatro dessas políticas, acolhidas no que se denomina "Programa Justiça 4.0", que são: o Juízo 100% Digital, os Núcleos de Justiça 4.0, o Balcão Virtual e a Plataforma Digital do Poder Judiciário.

O Juízo 100% Digital foi estabelecido pela Resolução CNJ n.º 345, de outubro de 2020, que determina a possibilidade de um procedimento judicial inteiramente virtual, ou seja, todos os atos processuais são praticados por meio eletrônico, inclusive audiências e sessões de julgamento, que devem acontecer por videoconferência, não necessitando, assim, de comparecimento das partes aos fóruns.

Destaca-se que o Juízo 100% Digital não é obrigatório, mas opcional, isto é, todas as partes devem concordar com a modalidade totalmente eletrônica, de acordo com os termos da Resolução CNJ n.º 345/2020, conforme artigo 3º[4].

A finalidade do Juízo 100% Digital, de acordo com o Conselho Nacional de Justiça (2022, p. 21) é: "garantir às pessoas que precisam da Justiça o direito fundamental de duração razoável dos processos, com mais celeridade, segurança, transparência, produtividade e acessibilidade, bem como promover a redução dos gastos públicos".

Os Núcleos de Justiça 4.0 foram criados de forma complementar ao Juízo 100% Digital, de acordo com a Resolução n.º 385, de abril de 2021, com competência para resolver conflitos de matérias específicas, também de maneira remota. Desse modo, cada

[4] Art. 3º A escolha pelo "Juízo 100% Digital" é facultativa e será exercida pela parte demandante no momento da distribuição da ação, podendo a parte demandada opor-se a essa opção até o momento da contestação. §1º A parte demandada poderá se opor a essa escolha até sua primeira manifestação no processo, salvo no processo do trabalho, em que essa oposição deverá ser deduzida em até 05 dias úteis contados do recebimento da primeira notificação. § 2º Adotado o "Juízo 100% Digital", as partes poderão retratar-se dessa escolha, por uma única vez, até a prolação da sentença, preservados todos os atos processuais já praticados. § 3º No processo do trabalho, ocorrida a aceitação tácita pelo decurso do prazo, a oposição à adoção do "Juízo 100% Digital" consignada na primeira manifestação escrita apresentada não inviabilizará a retratação prevista no §2º. (CNJ, 2020).

Núcleo de Justiça deve ser formado por no mínimo três juízes, com competência sobre toda a área territorial situada dentro dos limites da jurisdição do tribunal a que pertence.

A principal intenção através da criação dos Núcleos de Justiça 4.0, de acordo com o Conselho Nacional de Justiça (2021, p. 15), é:

> Qualificar as demandas nas varas de primeiro grau, hoje sobrecarregadas", especialmente nas unidades das comarcas do interior, onde "são raras as varas especializadas e a especialização acadêmica e funcional do(a) magistrado(a) responsável por processos judiciais que envolvem diferentes matérias.

A seu turno, o Balcão Virtual é um projeto regimentado pela Resolução CNJ n.º 372, de fevereiro de 2021, que tem como objetivo replicar, em ambiente virtual, o atendimento realizado no "balcão" das secretarias judiciais, cujo serviço foi suspenso durante a pandemia, de maneira que qualquer pessoa como o advogado, partes, peritos e interessados possam, no horário de atendimento ao público, tirar suas dúvidas junto à secretaria judicial sem precisar ir até ao fórum.

A Resolução n.º 372/2021 CNJ proporciona que os diferentes órgãos judiciais escolham a própria ferramenta de videoconferência para o atendimento remoto e também prevê a disponibilidade de *software* gratuito desenvolvido pelo próprio Conselho Nacional de Justiça.

A Plataforma Digital do Poder Judiciário foi criada pela Resolução CNJ n.º 335, em setembro de 2020, objetivando que sirva como instrumento de integração entre os variados tribunais brasileiros, onde os órgãos judiciais podem cooperar no desenvolvimento de ferramentas que auxiliem no exercício da atividade judiciária.

Uma das principais finalidades da Plataforma Digital do Poder Judiciário é unificar o trâmite processual de todos os órgãos judiciais brasileiros em torno do PJe, logo, destina-se a tornar o PJe cada vez mais moderno e adequado à cada órgão judicial, empregando tecnologias e recursos modernos como computação em nuvem, experiência do usuário, *user experience - UX* e a inteligência artificial.

O Conselho Nacional de Justiça, através do Programa "Justiça em Números 2023", informou o aumento significativo de demandas levadas ao Poder Judiciário após

a pandemia Covid-19, sendo o ano de 2022 destaque como o maior ponto da série histórica: em 12 meses, ingressaram 31,5 milhões de casos novos em todos os segmentos de Justiça, representando um crescimento de 10% em casos novos, sendo baixados 30,3 milhões de processos, um aumento de 10,8% em relação ao ano de 2021. (CNJ, 2023).

Durante o ano de 2022, o Índice de Produtividade dos Magistrados (IPM) aumentou em 10,7%, o que equivale a uma média de 7,1 casos solucionados por dia útil do ano, sendo baixados 1.787 processos por magistrado. Por conseguinte, a proporção de casos novos eletrônicos atingiu 99%, aumentando consideravelmente o acesso à justiça durante o ano de 2022, vez que em apenas um ano foram ajuizados 31 milhões de casos novos eletrônicos, sendo a tramitação eletrônica uma realidade em 87,3% das ações em andamento, possuindo tempo de tramitação reduzido em cerca de um terço na comparação com o período dos processos físicos (CNJ, 2023).

Conforme o Conselho Nacional de Justiça, a utilização dessas ferramentas digitais evidenciou agilidade e eficiência, vez que o Poder Judiciário, durante o período pandêmico, reagiu às restrições de funcionamento e protocolos sanitários, garantindo, dessa forma, o acesso à justiça a todos os cidadãos, e diante dos resultados positivos obtidos através da implementação das novas tecnologias, continuaram a ser adotadas mesmo após o fim da pandemia, para a garantia da efetividade de diversos princípios constitucionais fundamentais ligados aos trâmites processuais.

5 CONSIDERAÇÕES FINAIS

O presente artigo científico buscou demonstrar que as inovações tecnológicas implementadas pelo Poder Judiciário, especialmente durante o período pandêmico, passaram a ser utilizadas até mesmo após a superação da pandemia e funcionaram como grandes aliadas à efetivação do princípio basilar do acesso à justiça pelos cidadãos brasileiros, promovendo uma revolução digital nos processos e procedimentos, que passaram a ser, majoritariamente, eletrônicos.

Analisou-se o compromisso constitucional e principiológico com um processo célere e efetivo firmado pela Constituição da República Federativa do Brasil de 1988, sendo então desenvolvidas várias ferramentas digitais a fim de possibilitar o acesso à justiça em um tempo em que as medidas de restrições impediam a livre circulação das pessoas e os atos judiciais precisavam ser reinventados e adaptados para o ambiente virtual.

Nesse contexto, comprovada a utilidade e eficiência das tecnologias implementadas, permanece a renovação digital da instrução do processo civil pelos projetos e sistemas virtuais implementados, com audiências telepresenciais, Juízo 100% digital, a Plataforma Justiça 4.0, o Balcão Virtual e a citação por meio eletrônico, sempre respeitando os limites estabelecidos na Constituição da República Federativa do Brasil de 1988 acerca do devido processo legal, do contraditório, ampla defesa e isonomia.

Desse modo, observou-se que o Processo Judicial Eletrônico, sem dúvidas, é um grande avanço em relação ao procedimento judicial, pois proporciona benefícios em relação a muitos aspectos, conforme citados ao longo do artigo. Com a difusão do processo eletrônico, nota-se com clareza solar a facilidade de acesso ao judiciário, e, consequentemente, destaca-se como uma sociedade democrática aquela onde os cidadãos conseguem acessar, de maneira viável, o Poder Judiciário, para resolverem seus conflitos no momento que desejarem.

Logo, é indiscutível que a implantação e difusão do processo eletrônico por parte do avanço tecnológico ao encontro do processo judicial ampliou o acesso da população em geral ao judiciário, beneficiando cada vez mais a celeridade e a qualidade das decisões judiciais, assegurando assim a plena continuidade do Estado Democrático de Direito com todos os princípios e garantias a ele inerentes.

REFERÊNCIAS

ABRÃO, Carlos Henrique. **Processo Eletrônico**: processo digital. 3.ed. São Paulo: Atlas, 2011.

BARROSO, Luís Roberto. ***Constituição da República Federativa do Brasil Anotada***. São Paulo: Saraiva, 1998.

BRASIL. **Constituição da República Federativa do Brasil**. Brasília: Senado, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 14 set. 2023.

BRASIL. **Lei nº 11.419. Promulgada em 19 de dezembro de 2006.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11419.htm>. Acesso em: 15 set. 2023.

BRASIL. **Lei nº 13.105, de 16 de março de 2015. Código de Processo Civil.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13.105.htm>. Acesso em: 14 set. 2023.

CALMON, Petrônio. **Comentários à Lei de Informatização do Processo Judicial**: Lei nº 11.419, de 19 de dezembro de 2006. Rio de Janeiro: Forense, 2008.

CAPPELLETTI, Mauro; GARTH, Bryant G.; NORTHFLEET, Ellen Gracie. **Acesso à Justiça.** Porto Alegre: Fabris, 1988.

CONSELHO NACIONAL DE JUSTIÇA. **Justiça em Números 2023.** Disponível em: <https://www.cnj.jus.br/wp-content/uploads/2023/09/sumario-executivo-justica-em-numeros-200923.pdf>. Acesso em: 13 nov. 2023.

CONSELHO NACIONAL DE JUSTIÇA. **Relatório Anual da Ouvidoria do Conselho Nacional de Justiça 2020**. Brasília (DF): CNJ, 2021. Disponível em: <https://www.cnj.jus.br/wpcontent/uploads/2021/05/Relatorio_anual_da_Ouvidoria_do_CNJ_ 2020_diagramado.pdf>. Acesso em: 15 set. 2023.

CONSELHO NACIONAL DE JUSTIÇA. **Justiça em Números 2022**. Brasília (DF): CNJ,2022. Disponível em: < https://www. cnj.jus.br/wpcontent/ uploads/2022/09/justica-emnumeros-2022.pdf>. Acesso em: 15 set. 2023.

DELGADO, José Augusto. Acesso à justiça: um direito da cidadania. **Informativo Jurídico da Biblioteca Ministro Oscar Saraiva.** Brasília, v. 9, n. 2, 1997.

DIDIER JR., Fredie. **Curso de Direito Processual Civil**: introdução ao direito processual civil, parte geral e processo de conhecimento. 22. ed. Salvador: Juspodivm, 2020.

FEÓLA, Luís Fernando. **Prática Jurídica no Processo Judicial Eletrônico**: Tribunal de Justiça do Trabalho. São Paulo: LT1, 2014.

FILHO, J. C. D. A. A. **Processo Eletrônico e Teoria Geral do Processo**. 5. ed. São Paulo: Grupo Gen Editorial, 2015.

GOVERNO FEDERAL. **Painel Coronavírus Brasil. Óbitos Confirmados.** 2023. Disponível em: <https://covid.saude.gov.br/>. Acesso em: 18 set. 2023.

GRINOVER, Ada Pellegrini. Ações Coletivas. **O Acesso à Justiça no Ano 2000.** O processo civil contemporâneo. Luiz Guilherme Marinoni (org.). Curitiba: Juruá, 1994.

LEAL JÚNIOR, Cândido Alfredo Silva. **Texto Judiciário Eletrônico:** decidindo e escrevendo no novo processo eletrônico. Revista de Doutrina da 4ª Região, Porto Alegre, n. 37, ago. 2010. Disponível em: <http://www.revistadoutrina.trf4.jus.br/artigos/edicao037/candido_junior.html>. Acesso em: 15 set. 2023.

MARINONI, Luiz Guilherme; ARENHART, Sérgio Cruz; MITIDIERO, Daniel. **Curso de Processo Civil**: teoria do processo civil. 2. ed. São Paulo: Editora RT, 2017.

MIRANDA DE OLIVEIRA, Pedro. **Novíssimo Sistema Recursal.** 3. ed. Florianópolis: Empório do Direito, 2017.

NERY JUNIOR, Nelson. **Princípios do Processo Civil na Constituição Federal**. 6. ed. São Paulo: RT, 2000.

PASCHOAL, Thais Amoroso. Acesso à justiça, tecnologia e o nosso realismo esperançoso de cada dia. In: FUX, Ávila; Henrique; CABRAL, Tricia Navarro Xavier (coord). **Tecnologia e Justiça Multiportas**: Teoria e prática. São Paulo: Editora Foco, 2021.

SILVA LOPES, Leopoldo Fernandes da. **Processo e Procedimento Judicial Virtual:** Comentários à lei 11.419/06 e suas importantes inovações. Revista Jurídica, Porto Alegre, n° 353, 2007.

TRIBUNAL REGIONAL FEDERAL DA 5ª REGIÃO. **Sobre o Pje - Processo Judicial Eletrônico.** 2023. Disponível em: <https://www.trf5.jus.br/index.php/pje>. Acesso em: 18 set. 2023.

A RESPONSABILIDADE CIVIL APLICADA A AGENTES AUTÔNOMOS DE INTELIGÊNCIA ARTIFICIAL NO TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS

CIVIL LIABILITY APPLIED TO AUTONOMOUS ARTIFICIAL INTELLIGENCE AGENTS IN THE PROCESSING OF SENSITIVE PERSONAL DATA

Rackel Farias Madeira[1]

Anamaria Sousa Silva[2]

RESUMO: O presente artigo tem como objetivo analisar o tratamento atribuído pela Lei nº 13.709, de 14.8.2018 (Lei Geral de Proteção de Dados), bem como por legislações pátrias correlatas e posições doutrinárias diversas, à responsabilização civil atribuída a agentes autônomos de inteligência artificial (IA) no contexto da proteção de dados pessoais sensíveis. Através de pesquisa bibliográfica e análise documental, buscou-se identificar as lacunas legislativas mais relevantes na disciplina deste tópico, para, posteriormente, suscitar alternativas viáveis a seu preenchimento. Ao final, o estudo demonstrará quais modalidades de responsabilização civil poderão ser adotadas no intuito de contribuir à efetiva salvaguarda dos direitos individuais na era digital.

Palavras-chave: responsabilidade civil; inteligência artificial; sistemas autônomos; dados pessoais sensíveis; Lei Geral de Proteção de Dados (LGPD).

ABSTRACT: The present article aims to analyze the treatment provided by the Brazilian Law No. 13,709, dated August 14, 2018 (General Data Protection Law), as well as related Brazilian legislation and various theories regarding the civil liability assigned to

[1] Graduanda em Direito pela Universidade Federal do Maranhão (UFMA). Lattes: http://lattes.cnpq.br/1892241496943291.

[2] Doutorado em Direito - Cooperação Internacional - pela Universidade de Nagoya - Graduate School of International Development - Japão (2000) - l - revalidado pela Universidade Federal de Santa Catarina. Mestrado na mesma área - Universidade de Nagoya - Graduate School of International Development - Japão (1997), revalidado pela UFSC. Graduação em Direito pela Universidade Federal do Maranhão (1993) Professora visitante da Universidade Federal do Maranhão durante o período de 2001-2003. Professora-bolsista DCR - CNPq - nível 2A - na Universidade Federal do Maranhão durante o período de 2004-2006. Professora adjunta da Universidade Federal do Maranhão (UFMA). Doutora em Direito - Cooperação Internacional pela Universidade de Nagoya - Japão. Lattes: : http://lattes.cnpq.br/7633585207951429.

autonomous agents of artificial intelligence (AI) in the context of sensitive personal data protection. Through bibliographic research and documentary analysis, we sought to identify the most relevant legislative gaps in the regulation of this topic, with the subsequent proposal of viable alternatives for its addressing. In conclusion, this study will demonstrate which forms of civil liability may be adopted to contribute to the effective safeguarding of individual rights in the digital age.

Keywords: civil liability; artificial intelligence; autonomous systems; sensitivedata; Brazilian General Data Protection Law (LGPD).

1 INTRODUÇÃO

O estudo em questão pretende apresentar perspectivas de responsabilização civil de agentes autônomos de inteligência artificial (IA) frente à violação de diretrizes normativas fornecidas pela Lei Geral de Proteção de Dados (LGPD) em relação ao tratamento de dados pessoais sensíveis.

A relevância dessa investigação se perfaz na constatação de que a inteligência artificial constitui uma ferramenta cada vez mais recorrente no dia a dia do cidadão contemporâneo, seja na elaboração de conteúdo personalizado em redes sociais, realização de procedimentos médicos complexos e estabelecimento de padrões que permitem prever a rentabilidade de investimentos ou até mesmo quais localidades possuem maior probabilidade de serem afetadas por mudanças climáticas. Trata-se, portanto, de um advento tecnológico que encontra repercussões nas esferas pública e privada, de forma que cabe à ciência jurídica encontrar mecanismos de regulamentação de tais efeitos.

Dentre as possíveis questões carentes de tutela jurisdicional advindas da utilização da IA por empresas e instituições, pode-se destacar a coleta, o processamento e armazenamento de dados pessoais, vez que o manejo destes é sujeito às diretrizes estabelecidas pela LGPD. De fato, não obstante a referida lei enfatize a importância da adoção de medidas de segurança a fim de garantir a proteção da privacidade dos usuários, o conteúdo fornecido por estes é frequentemente instrumentalizado no intuito de aprimorar a inteligência artificial, incluindo potenciais dados pessoais sensíveis.

Para a finalidade desta pesquisa, serão considerados principalmente os agentes de inteligência artificial que correspondem a modelos de linguagem treinados a partir de grandes conjuntos de dados obtidos online (*large language models*, ou LLMs), como GPT-3, GPT-3.5 e GPT-4, desenvolvidos pelo laboratório de pesquisa OpenAI. Nesse contexto inserem-se os *chatbots* (a exemplo do ChatGPT) e o Auto-GTP, aplicativo que utiliza o sistema GPT-4 no intuito de desempenhar tarefas autônomas, sem necessidade de direcionamento por parte do usuário.

Desta feita, tomando por base as metodologias de pesquisa bibliográfica e análise documental, investigou-se a possibilidade de responsabilização civil do gerenciador de dados pessoais sensíveis a partir de diferentes visões, atribuídas, sobretudo, pela legislação pátria, europeia, projeto de lei em trâmite e posicionamentos doutrinários. Verifica-se que, no que pese o expressivo aumento de publicações nessa seara, restam lacunas normativas no ordenamento brasileiro em respeito à modalidade de responsabilização adotada.

Este estudo discute soluções introduzidas pelas fontes elencadas em diálogo com a LGPD, abordando decisões dos tribunais superiores pertinentes ao ponto, o Regulamento Geral de Proteção de Dados (RGPD), o Projeto de Lei n. 2.338/2023, posicionamentos recentes da Agência Nacional de Proteção de Dados (ANPD) e preceitos avindos das contribuições teóricas de Caitlin Mulholland e Walter Aranha Capanema, dentre outros.

2 AGENTES AUTÔNOMOS DE INTELIGÊNCIA ARTIFICIAL E DADOS PESSOAIS SENSÍVEIS EM FACE DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD): CONCEITOS FUNDAMENTAIS

Uma das definições mais célebres de inteligência artificial é a proposta por John McCarthy, um dos pioneiros da IA. Para McCarthy (1956), "inteligência artificial é a ciência e a engenharia de fazer máquinas inteligentes, especialmente programas de computador inteligentes". Esse entendimento foi difundido a princípio pelo cientista no artigo *"Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*",

publicado em 1956 e considerado um marco histórico da área por ter sido o primeiro a apresentar formalmente a ideia de que máquinas poderiam ser programadas para imitar a inteligência humana.

Décadas mais tarde, Andrew Ng introduziu uma delimitação mais atual para aprendizado de máquina (*machine learning*): “aprendizado de máquina é o campo de estudo que dá aos computadores a habilidade de aprender sem serem explicitamente programados" (NG, 2017).

Em outras palavras, inteligência artificial é uma área da ciência da computação que se dedica ao estudo e desenvolvimento de algoritmos e sistemas capazes de realizar tarefas que, tradicionalmente, exigem inteligência humana.

Por sua vez, agentes autônomos, segundo o entendimento de RUSSELL e NORVIG (2013, p. 35), são “entidades de software ou hardware que se movem em algum ambiente, percebem o ambiente por meio de sensores, agem no ambiente por meio de atuadores e podem operar sem intervenção humana direta".

Tais agentes utilizam técnicas de inteligência artificial para coletar informações, analisá-las e tomar decisões com base em regras e objetivos pré-definidos. Assim, são capazes de autoaprimoramento ao valer-se de estratégias como aprendizado de máquina, ajustes de algoritmos, avaliação de resultados e análise de dados.

De fato, para os autores supramencionados, “a análise de dados é o coração da inteligência artificial, permitindo que sistemas computacionais aprendam a partir de exemplos e experiências" (*Ibidem*, p. 17). Isso porque os algoritmos de *machine learning* analisam conjuntos de dados a fim de identificar padrões entre as variáveis presentes, a partir dos quais o algoritmo poderá inferir informações e fazer previsões sobre dados inéditos, não utilizados no treinamento do modelo.

Nesse cenário, dados precisam ser coletados, armazenados e processados em grande quantidade e qualidade, fazendo-se necessário que sejam representativos e variados o suficiente para que o modelo possa generalizar suas conclusões e fazer previsões precisas, então gerando novos dados.

Conquanto no contexto normativo brasileiro atual não exista uma lei em vigor que discipline exclusivamente o uso da inteligência artificial, a LGPD pode ser aplicada a algumas questões relacionadas ao seu uso, uma vez que estabelece regras para o tratamento de dados pessoais (incluindo aqueles que possam vir a ser utilizados por sistemas de inteligência artificial), exigindo que empresas obtenham consentimento do titular para coletar e tratar suas informações e que tomem medidas para garantir a segurança de dados.

A definição de dado pessoal consta no artigo 5º, inciso I, da LGPD, que dispõe: "dado pessoal: informação relacionada à pessoa natural identificada ou identificável". Do mesmo modo, comentam BLUM e RABELO (2020, p. 51):

> Dados pessoais são informações relacionadas a uma pessoa natural identificada ou identificável, como nome, endereço, número de telefone, número de CPF, informações de cartão de crédito, dados biométricos, informações de localização, registros de atividades de navegação na internet, informações de saúde, entre outras, desde que essas informações permitam a identificação ou possam tornar identificável a pessoa natural a quem se referem.

Logo, adota-se o entendimento de que dados pessoais são informações relacionadas à pessoa natural identificada ou identificável, direta ou indiretamente, por meio de identificadores como nome, número de identificação, endereço, dados de localização, dentre outros. O tratamento desses dados deverá ser realizado com o consentimento do titular ou em outras situações previstas em lei (conforme o art. 7º, inciso II, LGPD). Para mais, determina que isso ocorra de forma transparente e segura, garantindo a privacidade e proteção dos dados pessoais (art. 6º).

Por outro lado, a mesma lei estabelece, em seu artigo 5º, inciso II, que dados pessoais sensíveis

> [...] são dados pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

O conceito é também explorado por NASCIMENTO e PEREIRA (2020, p. 50), que elucidam:

> Dados pessoais sensíveis são aqueles que, em razão de sua natureza, estão associados a maior risco à privacidade ou geram maior impacto à esfera íntima das pessoas, tais como informações sobre saúde, orientação sexual, origem racial, convicções religiosas e filosóficas, dentre outras.

Dados pessoais sensíveis são, portanto, informações que, se indevidamente divulgadas ou utilizadas contra alguém, podem gerar prejuízos significativos a sua vida privada, dignidade e intimidade, sendo de suma importância sua proteção para garantir a autonomia dos titulares. Desta forma, a denominação utilizada ("sensíveis") advém do fato de que se forem manejados de forma imprópria, podem causar graves danos ao cidadão, como discriminação, estigma, exclusão social, perda de oportunidades e violação ao princípio da dignidade da pessoa humana.

Entendimento consonante é o de MUHOLLAND (2021, p. 02):

> Mais importante do que identificar a natureza própria ou conteúdo do dado - conforme o rol do artigo 5º. II, LGPD - é constatar a potencialidade discriminatória no tratamento de dados pessoais. Isto é, a limitação para o tratamento de dados se concretizaria na proibição de seu uso de maneira a gerar uma discriminação, um uso abusivo e não igualitário de dados.

Ilustrativamente, a autora citada narra casos em que o perfilamento (*profiling*) a partir do uso de dados pessoais sensíveis ocasionou tratamento discriminatório. Em um deles, ocorrido nos Estados Unidos,

> [...] algumas seguradoras utilizaram dados pessoais relacionados às vítimas de violência doméstica, acessíveis em banco de dados públicos. O resultado do tratamento dos dados levou a uma discriminação negativa, ao sugerir que mulheres vítimas de violência doméstica não poderiam contratar seguros de vida, saúde e invalidez.

Destarte, em face das possibilidades geradas pela utilização prejudicial desses dados pessoais, a LGPD estabelece mecanismos de proteção mais restritivos em relação

a outras modalidades de *data*, exigindo que empresas e organizações adotem medidas técnicas e administrativas adequadas e proporcionais ao risco envolvido.

No caso dos algoritmos autônomos de inteligência artificial, sua capacidade de coletar, armazenar e processar grandes quantidades de dados pessoais sensíveis os torna aptos a cometer violações de segurança, de forma que as medidas disciplinadas pela LGPD se tornam particularmente relevantes nesse contexto.

Tais medidas incluem a adoção de algoritmos de criptografia, o controle de acesso aos dados, a anonimização dos dados pessoais sensíveis e a realização de avaliações de impacto à privacidade, entre outras. Determina, ainda, que as empresas que utilizam inteligências artificiais informem aos titulares de dados como estes serão coletados, tratados e utilizados. Além disso, prevê que esses titulares terão direito a solicitar acesso, correção e exclusão de seus dados pessoais sensíveis coletados e tratados por meio de inteligências artificiais (arts. 6º a 30).

Observa-se, contudo, que, embora a LGPD evidencie a importância da efetiva proteção de dados pessoais sensíveis no contexto das inteligências artificiais, não há menção à imputação de responsabilidade civil a sistemas autônomos de inteligência artificial. A pauta, cuja relevância torna-se incontestável com a evolução exponencial do *machine learning* nos últimos anos, segue carente de regulação do legislador.

3 RESPONSABILIDADE CIVIL E A PROTEÇÃO DE DADOS PESSOAIS SENSÍVEIS

Com o avanço da tecnologia e o crescente uso de sistemas automatizados de processamento de dados, como inteligência artificial e *big data*, a responsabilidade civil pelos danos causados ao titular de dados adquire contornos notáveis. No tocante aos dados pessoais sensíveis, o motivo pelo qual essa discussão assume significado primordial possui relação com a natureza das informações compartilhadas, visto que tais dados tratam de elementos confidenciais e privados.

De acordo com DINIZ (2018, p. 36), “A responsabilidade civil é a aplicação de medidas que obriguem uma pessoa a reparar dano moral ou patrimonial causado a terceiros, em razão de ato por ela mesma praticado, por pessoa por quem ela responda, por alguma coisa a ela pertencente, ou de simples imposição legal”.

Em outras palavras, a responsabilidade civil é um instituto do direito civil que trata da obrigação legal de reparar os danos causados a terceiros, decorrentes de um ato ilícito. Essa obrigação decorre do princípio de que todo aquele que causa um dano a outrem deve repará-lo, independentemente da existência de culpa, e implica na obrigação de indenizar um terceiro pelos danos que lhe foram causados em decorrência de um comportamento que viole as normas jurídicas ou os princípios éticos. A ação judicial, nesse caso, busca a reparação integral do dano causado, incluindo o ressarcimento dos prejuízos materiais e a compensação pelos danos morais sofridos pela vítima.

No contexto da proteção de dados pessoais, a LGPD estabelece regras claras para a coleta, uso, armazenamento e compartilhamento destes pelas empresas e instituições públicas, atribuindo responsabilidades específicas aos controladores e operadores, que devem adotar medidas técnicas e organizacionais adequadas para proteção dessas informações. Assim, as empresas que tratam dados pessoais são responsáveis pelos danos que causarem, tanto na esfera material quanto moral, decorrentes de falhas de segurança, perda ou vazamento de informações. Isso implica que, em caso de violação, a empresa (ou instituição) pode ser obrigada a indenizar o titular dos dados por danos morais e/ou patrimoniais.

De fato, versa: "o controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo. (art. 42).”

Não obstante, a aplicação de multas em caso de descumprimento da LGPD está prevista no art. 52, que fixa a competência da Autoridade Nacional de Proteção de Dados (ANPD) para aplicar sanções administrativas, incluindo advertência, multa simples ou diária, bloqueio dos dados pessoais, eliminação dos dados, suspensão do exercício da

atividade de tratamento de dados pessoais e proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Ademais, essa legislação preconiza o direito dos titulares de dados pessoais a solicitar a reparação de danos causados por violações à lei, conforme estabelece o art. 5º, inciso V:

> O tratamento de dados pessoais deve ser realizado de forma transparente e com respeito às liberdades civis, aos direitos humanos e ao desenvolvimento econômico e tecnológico do país, nos termos desta Lei, em outras normas de proteção de dados pessoais e nas diretrizes da autoridade nacional. (...) VI - garantia da transparência no tratamento de dados, mediante informações claras e precisas sobre a realização do tratamento e os respectivos agentes, observados os segredos comercial e industrial.

Para mais, a supracitada lei estabelece a responsabilidade compartilhada entre controladores e operadores de dados pessoais, conforme anuncia o art. 42, parágrafo único: "O disposto no *caput* não exclui a responsabilidade solidária dos agentes de tratamento envolvidos, observados os artigos 23 a 25 desta Lei."

Quanto à natureza da responsabilidade civil decorrente do descumprimento da LGPD em relação a dados pessoais, há um debate em curso na doutrina jurídica. Isso porque, na realidade, a lei se limita a pontuar que “as hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente” (art. 45).

Nessa ótica, as normas da responsabilidade civil previstas na legislação em comento não possuem aplicação universal, uma vez que a sua incidência pode ser suplantada por normas específicas, tais como as disposições do Código de Defesa do Consumidor.

Justifica CAPANEMA (2020, p. 165):

> A responsabilidade surge do exercício da atividade de proteção de dados que viole a “legislação de proteção de dados”. Por essa expressão, o legislador reconhece que a proteção de dados é um microssistema, com normas previstas em diversas leis, sendo a LGPD a sua base estrutural. Deve-se aqui fazer uma analogia com o conceito de “legislação tributária” do art. 96 do CTN, para

> incluir não apenas as leis que versem sobre a proteção de dados, mas as normas administrativas regulamentares que serão expedidas pela Autoridade Nacional de Proteção de Dados ou por outras entidades.

Com efeito, embora a responsabilidade civil esteja regulamentada na Seção III do Capítulo VI da LGPD, denominada "Da Responsabilidade e do Ressarcimento de Danos", verifica-se que não há especificação de qual regime de responsabilidade civil deverá ser adotado.

Conquanto decisões recentes dos tribunais venham demonstrando a tendência do Judiciário de privilegiar a adoção do regime de responsabilização subjetiva, casos que envolvem proteção de dados pessoais vêm suscitando manifestações diversas. Como exemplo, o Acórdão da 27ª Câmara de Direito Privado do TJ/SP apreciou a Apelação Cível nº 1008308-35.2020.8.26.0704 de 16 de novembro de 2021, discutindo a responsabilidade civil por incidente de vazamento de dados pessoais não sensíveis a partir de uma perspectiva inédita, em que o Ministro relator Alfredo Attié, do Tribunal de Justiça do Estado de São Paulo (TJSP), elabora seu voto nos autos da AC 1008308-35.2020.8.26.0704:

> A respeito do regime de responsabilidade civil previsto na LGPD[...], não se trata mais, como antigamente, de aplicação das regras da responsabilidade subjetiva ou objetiva, mas sim do que a doutrina vem definindo como responsabilidade ativa ou proativa, hipótese em que, às empresas não é suficiente o cumprimento dos artigos da lei, mas será necessária a demonstração da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, a eficácia dessas medidas. (TJSP; Apelação Cível 1008308-35.2020.8.26.0704; Relator (a): Alfredo Attié; Órgão: 27ª Câmara de Direito Privado; Comarca de São Paulo; Data do Julgamento: 16/11/2021).

A concepção de que se trata de uma responsabilidade especial é reiterada por MORAES e QUEIROZ (2019, p. 113-136), que afirmam:

> Esta responsabilidade especial, à semelhança do que ocorre no Regulamento europeu, está articulada em torno de três noções fundamentais, que devem ser somadas: i) dano, ii) violação da legislação de proteção dos dados por parte do controlador e/ou operador e iii) reparação. Com efeito, o regime demanda que o dano seja resultante de violação da LGPD e que tenha sido causado por um

> agente de tratamento dos dados para então impor a obrigação de ressarcir a parte lesada. [...] A nova lei, porém, introduz, secundando o regulamento europeu, uma mudança profunda em termos de responsabilização. Trata-se da sua união ao conceito de "prestação de contas". Esse novo sistema de responsabilidade, que vem sendo chamado de "responsabilidade ativa" ou "responsabilidade proativa" encontra-se indicada no inciso X do art. 6º, que determina que às empresas que não é suficiente cumprir os artigos da lei; será necessário também "demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, a eficácia dessas medidas. Portanto, "não descumprir a lei, não é mais suficiente".

Infere-se, portanto, que a responsabilidade especial surge em substituição às regras da responsabilidade subjetiva ou objetiva. Neste regime de responsabilidade ativa (ou proativa), as empresas não podem se limitar ao cumprimento do texto legal, mas devem demonstrar a adoção de medidas eficazes que comprovem a observância e o cumprimento das normas de proteção de dados pessoais e sua eficácia. Essa responsabilidade especial está articulada em torno das noções fundamentais de dano, violação da legislação de proteção de dados e reparação.

Tal regime exige que o dano tenha sido resultado da violação da LGPD e causado por um agente de tratamento de dados para impor a obrigação de ressarcir a parte lesada. A legislação nacional introduz, em concordância com a europeia, uma profunda mudança em termos de responsabilização, unindo-a ao conceito de prestação de contas.

Realmente, a legislação de proteção de dados da União Europeia, conhecida como Regulamento Geral de Proteção de Dados (RGPD), estabelece princípios importantes relacionados à responsabilização pela proteção de dados pessoais, sendo os principais artigos que tratam desse assunto os de número 5 e 24.

Destaca-se, por exemplo, o Princípio da Integridade e Confidencialidade (art. 5.1.f), que assevera que "o responsável pelo tratamento deve garantir a segurança dos dados pessoais e protegê-los contra acesso não autorizado ou processamento ilegal". Por sua vez, o art. 24 estabelece a responsabilidade do encarregado pelo tratamento de dados pessoais ao afirmar que o responsável deve garantir que o tratamento conferido a eles esteja em conformidade com os princípios do RGPD, pugnando pela necessidade de programar medidas apropriadas para garantir o cumprimento das obrigações de proteção

de dados, incluindo a condução de avaliações de impacto da proteção de dados quando apropriado, paralelamente à designação de um encarregado de proteção de dados (DPO), quando necessário, e notificar violações de dados às autoridades competentes e às partes afetadas, caso aplicável.

Consequentemente, verifica-se que, para esse sistema de responsabilidade, a mera obediência à lei insuficiente.

Quanto a incidentes envolvendo dados sensíveis, o entendimento doutrinário dominante é de que a responsabilidade possui natureza objetiva (dano moral *in reipsa*). Ressalve-se, em todo caso, a existência de posições doutrinárias que preconizam a não diferenciação no regime de responsabilização por tratamento de dados pessoais, independentemente de serem estes sensíveis ou não. Compartilham dessa posição os juristas Caitlin Mulholland, Danilo Doneda e Rodrigo Gomes.

MULHOLLAND (2021, p. 11) justifica:

> [...] apesar do artigo 5º, II, da LGPD, trazer o conceito de dados sensíveis - exemplificado por um rol não taxativo, frise-se - deve-se considerar que o tratamento de dados que não estejam categorizados na lei como tal pode conduzir a resultados práticos discriminatórios, cujos efeitos a LGPD visa impedir justamente ao reconhecer e tutelar esta categoria de dados sensíveis. Isto é, a categoria de dados sensíveis não deve ser considerada como estruturalmente diversa da categoria de dados não sensíveis, na medida em que tanto uma, quanto outra estão sujeitas à potencialidade de tratamentos discriminatórios e geradores de danos a seus titulares. Sendo assim, não deve haver uma diferenciação de regimes de responsabilidade civil, baseada numa classificação dos dados como sensíveis ou não. Ou seja, o regime de responsabilidade civil adotado pela Lei Geral de Proteção de Dados Pessoais é único, independentemente da natureza do dado tutelado, se sensível ou não, pois a consequência de sua violação - o dano patrimonial ou moral, individual ou coletivo - independerá dessa categorização, devendo ser integralmente reparado.

Efetivamente, o art. 5º, II, da LGPD apresenta um rol não taxativo de dados sensíveis, de sorte que certas modalidades de tratamento de dados que não estão configuradas naquela Lei podem ser objetivo de responsabilização civil caso sua tutela ocasione resultados discriminatórios.

De todo modo, caso fosse adotada a responsabilização objetiva para dados sensíveis, deveria ser comprovado apenas o nexo causal entre a conduta e o dano, uma vez que o dano decorre de risco intrínseco à atividade desenvolvida pelo controlador. Igualmente, haveria necessidade de serem consideradas as implicações gravosas da utilização indevida das informações obtidas.

Com efeito, verifique-se o art. 6º, X, que traduz o princípio a responsabilização e prestação de contas, *in verbis*: "demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas".

Para MALDONADO e BLUM (2022),

> [...] é possível sustentar que a regra geral da LGPD é a responsabilidade civil subjetiva, na qual o elemento da culpa deverá ser demonstrado, admitida, em algumas hipóteses específicas, a responsabilidade civil objetiva, de acordo com a natureza da atividade de tratamento de dados pessoais, que realmente possa se enquadrar como atividade de risco.

Tendo em vista as possíveis consequências do manejo irresponsável de dados pessoais sensíveis, certamente que a atividade de tratamento destes se enquadraria em "atividade de risco". Nesse sentido vêm decidindo os tribunais, como se vislumbra no supracitado voto do Ministro relator Alfredo Attié, no qual exemplifica que: "[...] diferentemente seria a hipótese de vazamento de dados sensíveis, estes sim capazes de autorizar a condenação da ré por danos morais *in reipsa*, considerada a natureza dos dados violados".

Para fins deste estudo, compartilha-se da posição doutrinária que preceitua a responsabilização objetiva no contexto do tratamento de dados pessoais sensíveis, haja vista a natureza das informações manejadas.

4 LIMITES E ALCANCES DA PROTEÇÃO DE DADOS PESSOAIS SENSÍVEIS POR AGENTES AUTÔNOMOS DE INTELIGÊNCIA ARTIFICIAL

Em face das análises sustentadas até o presente momento, é possível tecer observações acerca de perspectivas de responsabilização civil de agentes autônomos de inteligência artificial. Nessa ótica, faz-se relevante, em princípio, discutir o que tal autonomia poderá significar para o direito.

RUSSEL e NORVIG (2013) explicam:

> A IA é autônoma quando pode tomar decisões sem intervenção humana. A autonomia pode se referir a tarefas específicas ou a um sistema que pode decidir a melhor forma de atingir um objetivo sem intervenção externa. A autonomia completa, em que a IA pode operar sem intervenção humana, é uma meta da pesquisa em IA, mas permanece inalcançável. (p. 11).

No que pese a visão desses pesquisadores, há de se ressaltar que durante os últimos anos verificou-se uma evolução exponencial das pesquisas referentes a IAs, de forma que o aprimoramento de modelos linguagem, como o mais recente de autoria da OpenAI, GPT-4 (Ope23), ensejam o vislumbre de inteligência artificial geral (AGI, ou *artificial general intelligence*), que é a capacidade de um agente inteligente alcançar habilidades cognitivas similares às de um ser humano.

De certo, o artigo "Sparks of Artificial General Intelligence: Early experiments with GPT-4", publicado em março de 2023, apresenta levantamentos baseados em experimentos que indicam uma evolução nesse sentido. Demonstra-se (BUBECK *et al*.):

> Pesquisadores em inteligência artificial (IA) têm desenvolvido e aprimorado grandes modelos de linguagem (LLMs) que apresentam notáveis capacidades em diversas áreas e tarefas, desafiando nossa compreensão de aprendizado e cognição. O mais recente modelo desenvolvido pela OpenAI, o GPT-4, foi treinado utilizando uma escala sem precedentes de poder computacional e dados. Neste artigo, relatamos nossa investigação sobre uma versão inicial do GPT-4, quando ainda estava em desenvolvimento ativo pela OpenAI. Argumentamos que esta versão inicial do GPT-4 faz parte de uma nova coorte de LLMs (junto com o ChatGPT e o PaLM da Google, por exemplo) que exibem uma inteligência mais geral do que os modelos de IA anteriores. Discutimos as crescentes capacidades e implicações desses modelos. Demonstramos que, além de sua maestria na linguagem, o GPT-4 pode resolver tarefas novas e difíceis que abrangem matemática, programação, visão, medicina, direito, psicologia e mais, sem a necessidade de estímulos especiais. Além disso, em todas essas tarefas, o desempenho do GPT-4 é impressionantemente próximo do desempenho humano e frequentemente

> ultrapassa significativamente modelos anteriores, como o ChatGPT. Dada a amplitude e profundidade das capacidades do GPT-4, acreditamos que ele poderia ser razoavelmente considerado uma versão inicial (embora ainda incompleta) de um sistema de inteligência artificial geral (IAG). Em nossa exploração do GPT-4, damos ênfase especial à descoberta de suas limitações e discutimos os desafios futuros para avançar em direção a versões mais profundas e abrangentes do IAG, incluindo a possível necessidade de buscar um novo paradigma que vá além da previsão da próxima palavra. Concluímos com reflexões sobre as influências sociais do recente salto tecnológico e as direções futuras de pesquisa. *(Tradução nossa*).

Partindo de análises similares, o jurista francês BAVAREZ (2023, n.p) prevê:

> O robô de conversação da OpenAI, ChatGPT, está revolucionando o cenário global ao democratizar o acesso à inteligência artificial com uma velocidade de desenvolvimento e disseminação sem precedentes. Apenas quatro meses se passaram entre o seu lançamento e a disponibilização no mercado da versão GPT-4, que já conta com mais de 100 milhões de usuários em todos os continentes. Prevê-se que esta seja substituída pela versão GPT-4.5 a partir de setembro, seguida por uma inteligência artificial integral anunciada para 2025. Esta última poderá não apenas superar a capacidade humana na busca por informações e conhecimento, bem como na produção de conteúdo, mas também rivalizar em termos de raciocínio e inovação.

Tais considerações acerca da autonomia da inteligência artificial importam às ciências jurídicas, visto que a possibilidade de responsabilização civil desses agentes depende da interpretação a eles dada enquanto objeto ou sujeito de direitos.

Para estudiosos que consideram IAs objetos de direito, criados e controlados por seres humanos, esses sistemas não possuem autonomia ou capacidade de tomar decisões independentes, tornando-os inaptos a serem sujeitos de direito. Um exemplo de posição nessa linha de raciocínio é apresentado por DANAHER (2018):

> Deveríamos considerar as IAs como sujeitos legais, mas não como personalidades jurídicas. Não devemos ser tão precoces em conceder aos sistemas de IA a gama completa de direitos legais que normalmente concedemos a pessoas naturais, pois fazê-lo ignoraria as diferenças muito reais e significativas entre seres humanos e sistemas de IA. (*Tradução nossa*).

Por outro lado, abordagens que sustentam que inteligências artificiais devem ser consideradas sujeitos de direito (ou seja, entidades autônomas e capazes de tomar

decisões independentes) alegam que esses agentes possuem uma forma de personalidade jurídica, com direitos e deveres próprios. Esse posicionamento é defendido, por exemplo, por CALO (2017), que leciona:

> Se continuarmos a tratar a IA como mera propriedade, estaremos limitando seu potencial e deixando de abordar as implicações éticas e sociais de seu uso. Precisamos começar a considerar as IAs como entidades que possuem interesses e direitos próprios, e que podem ser responsabilizadas por suas ações. (*Tradução nossa*).

De toda sorte, as atuais teorias de responsabilização civil desses agentes partem da premissa de que se tratam de objetos (e não sujeitos) de direito, podendo ser equiparados a coisas inanimadas, ainda que apresentem certo grau de autonomia. Esse raciocínio decorre, principalmente, da obrigatoriedade de intervenção humana para possibilitar processos de aprendizado a partir dos quais os dados serão manejados, justificando que a responsabilidade seja imputada aos envolvidos, já que tais ações, conforme o exposto, ainda precisam ser guiadas, mesmo que a princípio.

Dito isto, embora não mencione expressamente a IA, o art. 20 da LGPD trata do direito de revisão de decisões baseadas em tratamentos automatizados de dados pessoais ao dispor que "o titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais [...]", o que inclui processos resultantes de *machine learning*. A despeito dessa menção, porém, não consta naquela legislação uma caracterização do que se entende por decisões automatizadas, possibilitando que tal terminologia abarque diversos outros cenários.

Para LIMA e SÁ (2020, p. 231),

> A reflexão sobre a discriminação é atual e relevante, pois os sistemas de IA estão sendo utilizados, em muitos países, com os mais diversos objetivos. Exemplo é o policiamento preditivo que, mediante a análise de dados disponíveis, busca prever onde o crime poderá ocorrer. Ocorre que os sistemas de predição e outros sistemas de IA não estão livres de distorções no resultado. Afinal, os dados são inseridos por programadores humanos que, mesmo involuntariamente, podem contaminá-los com seus preconceitos. A LGPD não discrimina as hipóteses em que o processamento totalmente automatizado de dados pode ocorrer. Limita-se a disciplinar o direito à explicação quando a

> decisão automatizada é tomada sem qualquer interferência humana. Assim, o tratamento de dados automatizados submete-se às regras gerais de utilização e tratamento de dados, especialmente aquelas previstas nos arts. 7º e 11.

Com efeito, não obstante as situações descritas encontrem equivalente nas consequências da utilização da inteligência artificial em tempos presentes, o excesso de generalidade com que a norma trata a automatização do processamento de dados poderia criar empecilhos à correta adequação dessas ocorrências ao texto normativo.

Em contrapartida, o recém-introduzido Projeto de Lei n. 2.338/2023 (PL nº 2.338/2023), que visa disciplinar acerca do uso das inteligências artificiais, inclui o direito de revisão de decisões automatizadas, abarcando "não apenas situações nas quais os interesses das pessoas são afetados – como também ocorre na LGPD –, mas também em casos nos quais o uso de sistemas de IA produzam efeitos jurídicos relevantes" (ANDP, 2023). O ponto de sobreposição, assim, reside justamente nos casos em que IAs venham a realizar tratamento de dados pessoais.

Cabe ressaltar que o projeto de lei entende tal responsabilização como princípio do "desenvolvimento, implementação e uso dos sistemas" (BRASIL, 2023), que deverão observar a boa-fé e, dentre outros, a "rastreabilidade das decisões durante o ciclo de vida de sistemas de inteligência artificial como meio de prestação de contas e atribuição de responsabilidades a uma pessoa natural ou jurídica" e a "prestação de contas, responsabilização e reparação integral de danos" (*Ibidem*).

De fato, a integralidade do Capítulo V, do PL nº 2.338/2023, é dedicada à responsabilidade civil dos agentes de inteligência artificial, associando os danos por estes causados à necessidade de reparação integral "independentemente do grau de autonomia do sistema". Em relação à modalidade de responsabilização aplicada, consta (art. 27):

> § 1º Quando se tratar de sistema de inteligência artificial de alto risco ou de risco excessivo, o fornecedor ou operador respondem objetivamente pelos danos causados, na medida de sua participação no dano.
> § 2º Quando não se tratar de sistema de inteligência artificial de alto risco, a culpa do agente causador do dano será presumida, aplicando-se a inversão do ônus da prova em favor da vítima. (p. 19).

Trata-se de uma adaptação da teoria do risco (teoria da responsabilização objetiva), similarmente ao que consta no parágrafo único do art. 927 do Código Civil, que versa: "haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem".

Assim, o PL nº 2.338/2023 preconiza que a natureza da responsabilidade do sistema de inteligência artificial depende de análise prévia da amplitude dos riscos apresentados por sua utilização, podendo ser objetiva ou não. Não o sendo, aplicar-se-á a inversão do ônus da prova em favor da vítima, conclusão que poderia advir do pressuposto de que o usuário é a parte vulnerável na relação, em paralelo ao que ocorre no Direito do Consumidor (arts. 4º c/c 6º, inciso VIII, do Código de Defesa do Consumidor [CDC]).

Quanto às hipóteses de não responsabilização (art. 28),

> Os agentes de inteligência artificial não serão responsabilizados quando:
> I – comprovarem que não colocaram em circulação, empregaram ou tiraram proveito do sistema de inteligência artificial; ou
> II – comprovarem que o dano é decorrente de fato exclusivo da vítima ou de terceiro, assim como de caso fortuito externo. (p. 20).

No tocante às hipóteses de responsabilização civil de sistemas autônomos de inteligência artificial por danos causados no âmbito das relações de consumo, o art. 29 preceitua a aplicação concomitante do CDC e do PL nº 2.338/2023.

Conquanto a atribuição de papel jurídico a tais regras sanaria certas questões relativas à atribuição de responsabilidade a esses agentes por ocasião do manejo de dados pessoais sensíveis, haveria confronto entre as abordagens apresentadas por LGPD (mais geral) e PL (mais específico).

Observe-se, contudo, que o princípio da especialidade se aplica quando mais de uma norma incide sobre o mesmo fato jurídico, tal que a norma especial afasta a incidência de norma geral (*lex specialis derogat legi generali*). No tocante ao regime de

responsabilização, a norma especial em questão (PL) contém os elementos da geral (LGPD), acrescida de pormenores que particularizam o fato.

Destarte, eventual aprovação e implementação das regulações contidas no PL nº 2.338/2023 poderia apresentar uma solução aparente ao problema da lacuna existente nesse âmbito, desde que observadas as diretrizes de proteção de dados preconizadas pela LGPD, desta feita aplicadas aos sistemas de inteligência artificial.

5 CONSIDERAÇÕES FINAIS

Embora a Lei Geral de Proteção de Dados (LGPD) tenha recebido notável contribuição do direito europeu, cabe relembrar que sua temática apenas na última década encontrou as primeiras reverberações no direito positivo nacional, sendo a própria publicação da legislação em comento datada de 14 de agosto de 2018, tendo entrado em vigor em setembro de 2020.

Com o crescimento de aplicações da inteligência artificial no dia a dia do brasileiro, além do consequente aumento do volume de dados manejados, observou-se o surgimento de adventos tecnológicos alheios à criatividade do legislador no momento da elaboração de tais instrumentos normativos, torna-se inevitável, em certa medida, que estes venham a apresentar lacunas, haja vista a impossibilidade de contemplação de aspectos ainda por emergir.

Contudo, em homenagem ao princípio da segurança jurídica, não é razoável que o titular de dados se encontre desprotegido frente a essas mudanças. Ressalte-se que, em se tratando de dados pessoais sensíveis, a vulnerabilidade do titular é especialmente evidenciada pelo conteúdo das informações e os efeitos que sua utilização irresponsável poderia causar.

Baseado nos resultados obtidos através da presente pesquisa e uma vez conceituados os temas congruentes, foram identificadas as principais propostas de responsabilização civil pelo manejo de dados pessoais sensíveis por parte de algoritmos autônomos de inteligência artificial. Argumentou-se em favor da responsabilização

objetiva (adoção da teoria do risco), em consonância com a doutrina majoritária vigente. Discutiu-se a abordagem introduzida pelo PL nº 2.338/2023, posicionando-o enquanto possível instrumento normativo futuro voltado à disciplina do tópico, embora apresente pontos controvertidos em relação à LGPD.

Evidenciou-se, por fim, que a disciplina formal da responsabilização civil dos sistemas supramencionados é não apenas possível, mas imperiosa, e poderia, em certa medida, ser alcançada a partir da adoção conjunta do PL nº 2.338/2023 (caso este venha a se transformar em Lei) e da LGPD, acrescidos de adequações.

REFERÊNCIAS

ALBIANI, Christine. **Responsabilidade Civil e Inteligência artificial**: Quem responde pelos danos causados por robôs inteligentes? Disponível em: https://bit.ly/3AtutOB. Acesso em: 25 abr. 2023.

ANPD. **Análise preliminar do Projeto de Lei nº 2338/2023, que dispõe sobre ouso da Inteligência Artificial**. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/analise-preliminar-do-pl-2338_2023-formatado-ascom.pdf. Acesso em: 08 out. 2023.

BAZZAN, Ana Lucia; LABIDI, Samira. **Agentes autônomos**: uma introdução. Porto Alegre: Sociedade Brasileira de Computação, 2003, p. 17-31.

BAVAREZ, Nicolas. **La révolution ChatGPT**. Disponível em: https://www.lefigaro.fr/vox/societe/nicolas-baverez-la-revolution-chatgpt-20230416. Acesso em: 04 maio. 2023.

BRASIL. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Lei nº 13.709, de 14 de agosto de 2018.

BRASIL. **Projeto de Lei N° 2338, de 2023.** Disponível em: https://shre.ink/nsFe. Acesso em: 07 out. 2023.

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Editora Forense, 2021.

BUBECK, Sébastien *et al*. **Sparks of Artificial General Intelligence**: Early experiments with GPT-4. Disponível em: https://doi.org/10.48550/arXiv.2303.12712. Acesso em: 01 maio 2023.

CALO, Ryan, **Artificial Intelligence Policy**: A Primer and Road map. 07 ago. 2017.Disponível em: https://ssrn.com/abstract=3015350. Acesso em 03 maio 2023.

CAPANEMA, Walter Aranha. A responsabilidade civil na Lei Geral de Proteção de Dados. In: **Cadernos Jurídicos**, n. 53, p. 163-170, 2020. Disponível em: https://bit.ly/3oRhAv9. Acesso em: 30 abr. 2023.

CHESTERMAN, Simon. Artificial Intelligence and The Limits of Legal Personality. In: **International & Comparative Law Quarterly**, 69(4), 819-844, 2020. Disponível em: https://bit.ly/3LB9ZIU. Acesso em: 30 abr. 2023.

DINIZ, Maria Helena. **Curso de Direito Civil Brasileiro**. São Paulo: Saraiva, 2018.

JORDAN, Michael; MITCHELL, Thomas. Machine learning: Trends, perspectives, and prospects. In: **Science**, n. 349, p. 255-260, 2015. Disponível em: https://doi.org/10.1126/science.aaa8415. Acesso em 22 abr. 2023.

LIMA, Taisa Maria Macena de; SÁ, Maria de Fátima Freire de. Inteligência Artificial e Lei Geral de Proteção de Dados Pessoais: O Direito à Explicação nas Decisões Automatizadas. In: **Revista Brasileira de Direito Civil**. Belo Horizonte, v. 26, p. 227-246, out./dez. 2020.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD**: Lei Geral de Proteção de Dados Pessoais Comentada. 4 ed. Rio de Janeiro: Revista dos Tribunai, 2022.

MCCARTHY, John. **Proposal for the Dartmouth Summer Research Project on Artificial Intelligence**. Disponível em:https://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf. Acesso em: 23 abr. 2023.

MORAES, Maria Celina Bodin de; QUEIROZ, João Quinelato de. Autodeterminação informativa e responsabilização proativa: novos instrumentos de tutelada pessoa humana na LGPD. In: **Cadernos Adenauer**, ano XX, vol. 3, 2019.

MULHOLLAND, Caitlin. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). In:**Revista de Direitos e Garantias Fundamentais**, v. 19, 2018.

MULHOLLAND, Caitlin. Responsabilidade civil por danos causados pela violação de dados sensíveis e a Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018). In: **IBERC**: Instituto Brasileiro de Estudos de Responsabilidade Civil, 2021. Disponível em: https://bit.ly/3nf7DaI. Acesso em: 01 maio 2023.

NASCIMENTO, Juliana Abrusio; PEREIRA, Bianca Dazzi. **Proteção de Dados Pessoais e a Lei Geral de Proteção de Dados**: desafios e perspectivas. Belo Horizonte: D'Plácido, 2020.

NG, Andrew. **Wha tis Machine Learning?** Disponível em: https://www.youtube.com/watch?v=LOuGmwpS01A. Acesso em: 23 abr. 2023.

RUSSELL, Stuart Jonathan; NORVIG, Peter. **Inteligência artificial**. Rio de Janeiro: Elsevier, 2013.

STANCIOLI, Brunello Souza; LOPES, Giovana Figueiredo Peluso. A personificação de agentes autônomos de inteligência artificial. In: **Revista de direito civil contemporâneo**. n. 23, p. 65-93, abr./jun, 2020. Disponível em: https://dspace.mj.gov.br/handle/1/3310. Acesso em 21 abr. 2023.

TJS. **Apelação Cível 1008308-35.2020.8.26.070**. Relator (a): Alfredo Attié; Órgão: 27ª Câmara de Direito Privado; Comarca de São Paulo; Data do Julgamento: 16/11/2021. Disponível em: https://images.jota.info/wp-content/uploads/2022/05/20210000929192.pdf. Acesso em: 26 abr. 2023.

UNIÃO EUROPEIA. **Regulamento Geral sobre a Proteção de Dados**. 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT. Acesso em: 02 maio 2023.

A NOVA TECNOLOGIA BLOCKCHAIN: A REVOLUÇÃO NO MUNDO JURÍDICO

THE NEW BLOCKCHAIN TECHNOLOGY: THE REVOLUTION IN THE LEGAL WORLD

Silvana Porciuncula de Moraes[1]

Luciana Picanço de Oliveira[2]

RESUMO: A pesquisa científica na área jurídica, cuja metodologia de estudo é qualitativa e bibliográfica, tem como objetivo identificar o potencial de uma ferramenta tecnológica que tem aguçado a curiosidade do mundo corporativo, devido ao seu diferencial em prevenir fraudes, furto de dados – seja através da prática de *phishing*, ou ataques de *ransomware*- e invasão de privacidade ocorridos no mundo virtual, além de possibilitar a criação de diferentes modelos de negócios através de "Contratos Inteligentes" autoexecutáveis. Trata-se da tecnologia *Blockchain* que tem levantado vários questionamentos que serão objeto da pesquisa deste artigo, cujo objetivo é analisar o uso do "protocolo da confiança", como é conhecido o *Blockchain*, para atender demandas do mercado com relação à efetividade da segurança, privacidade e transparência num ambiente virtual. Ao longo da pesquisa está demonstrada a existência de uma tecnologia que tem impactado positivamente o mercado e o mundo jurídico. Dentro desse contexto, este trabalho se propõe a explorar o conhecimento e possibilidades de uso de uma tecnologia que tem abalado o mundo.

Palavras-chave: Blockchain; Contratos Inteligentes; Inovação Tecnológica; LGPD; Segurança.

ABSTRACT: Scientific research in the legal area, whose study methodology is qualitative and bibliographic, aims to identify the potential of a technological tool that has sharpened the curiosity of the corporate world, due to its differential in preventing fraud, data theft - either through practice of phishing or ransomware attacks - and invasion

[1] Mestranda em Propriedade Intelectual e Transferência de Tecnologia para Inovação na UFRJ-Profnit. Pós-graduada em Direito Digital pelo IERBB/MPRJ. Bacharel em Direito pela FACHA. Graduanda em Ciências Ambientais pela UNIRIO. Especialista em registro de marcas. Lattes: http://lattes.cnpq.br/3092334360125175.

[2] Doutoranda em Direito, instituições e negócios na UFF. Mestre em Direito, políticas públicas e sustentabilidade pela UNIRIO. Especialista em Direito Processual Civil pela UCAM. Lattes: http://lattes.cnpq.br/6740475699462348.

of privacy that occurred in the virtual world, in addition to enabling the creation of different business models through self-executing "Smart Contracts". This is the Blockchain technology that has raised several questions that will be the object of this article's research, whose objective is to analyze the use of the "trust protocol", as Blockchain is known, to meet market demands regarding the effectiveness of security, privacy and transparency in a virtual environment. Throughout the research, it is demonstrated the existence of a technology that has positively impacted the market and the legal world. Within this context, this work proposes to explore the knowledge and possibilities of using a technology that has shaken the world.

Keywords: Blockchain; Smart Contracts; technological innovation; LGPD; Security.

1 INTRODUÇÃO

O mundo corporativo tem se deparado, a cada dia, com novos desafios em relação a segurança de dados que, nos dias de hoje, são considerados o novo petróleo. Portanto, tem se intensificado a adoção de sistemas de gestão de segurança da informaçãopara garantir a confidencialidade, disponibilidade, autenticidade, integridade e legalidade dos dados transacionados. A complexidade em identificar soluções inovadoras tem sido o grande desafio nas corporações, e as empresas têm buscado investir em tecnologia de ponta como sendo uma alternativa inteligente para zelar pela segurança e integridade dos dados, além de ajudar a manter as empresas em conformidade com a Lei 13.709/2018– LGPD (BRASIL, 2018).

Os dados são considerados os ativos da empresa, com valores imensuráveis. Portanto, preservá-los é a missão de todas as empresas que têm como meta garantir a sua segurança.

As empresas têm se conscientizado sobre a importância e urgência de investir em novas tecnologias com o objetivo de prevenção contra o vazamento de dados pessoais, sensíveis e estratégicos e, consequentemente, evitar perdas econômicas oriundas de falhas de segurança de suas informações.

O mundo está cada vez mais digital, com a evidência de contratos assinados virtualmente, das transações comerciais, como *e-commerce*, serviços de táxi, de

restaurantes, dentre outros serviços, ao serem transacionados digitalmente, agilizando, dessa forma, na prestação de serviços. Vale ressaltar que, sem os dados, não se consegue fazer nada.

Uma das contribuições na mudança da forma de contratação, são as moedas digitais que já se tornaram uma realidade e, portanto, têm revolucionado o sistema financeiro através de transações sem a necessidade de intermediários, com o advento da nova tecnologia *Blockchain*. Tecnologia, esta, que tem proporcionado mudanças nos negócios jurídicos, no quetange à validação das transações financeiras. Mas, diversos serviços podem se beneficiar ao adotar a tecnologia *Blockchain*, seja para negociação de contratos, licitação, registro de documentos públicos e privados, investir no mercado financeiro, dentre outros usos importantes que têm agregado valor numa sociedade que está caminhando para um mundo digital.

A segurança, integridade dos dados, a imutabilidade, rastreabilidade, com rede distribuída e privacidade, proposta pela tecnologia *Blockchain* é o que tem chamado a atenção das empresas que, inclusive, já estão investindo na implementação da tecnologia para seu uso em potencial, com fins de proporcionar um serviço que impede a ocorrência de fraudes. Tamanha inovação é o objeto do presente trabalho, tratando-se de uma ferramenta com alto potencial para a reduçãoda judicialização e das perdas econômica e reputacional.

A tecnologia *Blockchain* vem sendo adotada por todo o mundo. Em consonância com as transações globais, o sistema jurídico brasileiro vem adotando o registro de provas em *Blockchain*, por identificar o seu potencial probatório. Assuntos como corrupção, lavagem de dinheiro, roubo e furto são amparados pelo direito penal; contratos, negociações, acordos, parcerias são amparados pelo direito civil e empresarial; impostos e tributação no meio digital, liderado pelo direito tributário; registro de marcas e patentes amparados pelo direito de propriedade industrial, dentre outras matérias, podem se beneficiar da tecnologia Blockchain, por seus inúmeros benefícios, tais como: da imutabilidade, rastreabilidade, transparência e segurança.

A pesquisa proposta é qualitativa sob o método analítico. Será realizado um estudo bibliográfico, com análise de documentos com o fulcro de aprofundar os desafios na segurança de dados no mundo corporativo e as vantagens da adoção da *Blockchain* e dos *Smart Contracts* nos contratos empresariais. Portanto, será apresentado como resultado ao longo da pesquisa as evidências sobre a importância em investir nas novas tecnologias, com fins de aumentar a segurança das informações veiculadas no ambiente virtual e evitar vazamento de dados e, consequentemente, aumentar a segurança jurídica mediante a utilização da *Blockchain* e dos *Smart Contracts*.

2 SEGURANÇA DA INFORMAÇÃO E A LGPD

A Segurança da Informação (SI) já é uma prática adotada pelas corporações que se dedicam empreservar as informações da empresa. SI é requisito necessário para as empresas que desejam proteger sua integridade, confidencialidade, disponibilidade, autenticidade e legalidade – pilares garantidos pela segurança da informação.

A integridade é a garantia de que a informação não será manipulada nem alterada. A confidencialidade garante que somente as pessoas autorizadas tenham acesso à informação. A disponibilidade é a garantia de que a informação estará acessível mediante plano de recuperação de dados, em caso de desastre, para que não haja interrupção dos negócios. A autenticidade garante que as pessoas envolvidas em ações relacionadas a dados pessoais sejam identificadas por mecanismo como assinatura digital ou biometria – recursos tecnológicos (DONDA, 2020, p.36). A legalidade garante que o tratamento de dados pessoais ou dados sensíveis estejam em conformidade com a nova Lei no 13.709/18 - Lei Geral de Proteção de Dados Pessoais, conhecida por LGPD (BRASIL, 2018).

Com o advento da promulgação da nova Lei de proteção de dados pessoais, as empresas tiveram que se adequar a esta nova Lei e realinhar o trabalho da equipe de Segurança da Informação. Até então, a estratégia era preservar os dados empresariais, com informações estratégicas das empresas. Com a nova Lei, a estratégia teve que ser

realinhada incluindo, também, a proteção de dados pessoais, como forma de se adequar à nova exigência legal.

As empresas continuam em busca de esclarecimentos para se adequarem à nova Lei, a fim de atender aos requisitos legais e, consequentemente, aplicá-los na prática. Estar em conformidade com a LGPD requer conhecimento e investimento, sendo a tecnologia uma aliada para atender aos requisitos legais.

As melhores práticas de segurança de informação no tratamento de dados pessoais são adotadas pelas empresas, com o apoio jurídico que tem um papel fundamental com relação à forma de como os dados serão coletados, além de fazer a revisão e adequação dos contratos, política de segurança da informação, política de privacidade, e elaboração dos termos de consentimento.

A política de segurança da informação é um dos documentos importantes para nortear as empresas sobre como proteger as informações, e também é utilizada nas campanhas de conscientização junto aos colaboradores da empresa.

Como se pode observar, a LGPD provocou um maior impacto no ambiente da Segurança da Informação, que tem uma relevância nesse processo de adequação à Lei em questão. Para que as empresas implementem um sistema eficaz de gestão de segurança da informação, é necessário seguir as normas da ABNT NBR ISSO/IEC 27000, aliada à tecnologia para a coleta, processamento, compartilhamento, armazenamento e modificação ou eliminação dos dados. Portanto, a proteção de dados é um direito fundamental do cidadão.

> Art. 47 da Lei 13.709/2018, LGPD - Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término. (BRASIL, 2018).

O desafio de segurança da informação na era digital está relacionado com a proteção de informações, sejam dados pertencentes a indivíduos e/ou organizações. A norma ISO 27002 (2022) diz que “a segurança da informação é alcançada pela

implementação de um conjunto adequa do de controles, incluindo políticas, processos, procedimentos, estrutura organizacionale funçõesde software e hardware."

Por conseguinte, a proteção à privacidade depende do sistema de tecnologia da informação, depráticas negociais e de uma tecnologia de ponta para atender às demandas de mercado.

Segurança é um fator relevante quando se fala em LGPD, sendo, também, um fator decisivo na contratação de fornecedores de serviços. Existem dois protagonistas importantes no processo de proteção de dados: o Controlador dos dados pessoais, e o Operador, que provê os serviços contratados pelo Controlador. Ambos são considerados[3] agentes de tratamento de dados pessoais – de acordo com o artigo 5º., incisos VI e VII – Lei no.13.709/2018.

Como se sabe, inexiste um ambiente virtual 100% seguro, mas existem várias medidasde prevenção e de mitigação com vistas a evitar a exposição ilícita de dados. Portanto, quandoocorre o vazamento de informações, suas consequências levam às perdas econômicas ereputacionais das empresas.

De acordo com a renomada empresa americana, prestadora de serviços de tecnologia, "*The Ame Group*", é crucial manter os dados da empresa bem protegidos para evitar as consequências, fruto de violações de dados, tais como perda de receita e danos à reputação da marca. Adicionalmente, diz que:

> Na verdade, 93% das violações de dados bem-sucedidas ocorrem em menos de um minuto. Ainda assim, 80% das empresas levam semanas para perceber que ocorreu uma violação. (THE AME GROUP, 2023,n.p).

Quando ocorre o vazamento de dados, a sociedade entende como ausência de compromisso empresarial acerca da segurança dos dados e de sua conformidade com a Lei LGPD –gerando descrédito da figura empresarial, e ferindo a sua idoneidade, - o que

[3] Art 5º. VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competemas decisões referentes ao tratamento de dados pessoais; VII - operador: pessoa natural ou jurídica, de direito público ou privado,que realiza o tratamento de dados pessoais em nome do controlador.

resulta na perda econômica e reputacional.

O cliente valoriza sua privacidade e, geralmente, as violações envolvem informações pessoais, sensíveis e estratégicas de clientes. Consequentemente, a violação de dados leva à quebra de confiança de seus clientes.

Uma das preocupações das empresas, com relação à conformidade à LGPD, são os ataques cibernéticos com furtos de dados para fins ilícitos. Os crimes cibernéticos estão cada vez maissofisticados, tornando essencial a adoção de medidas preventivas e protetivas pelos profissionaisde Segurança de Informação.

De acordo com o relatório de segurança digital do Brasil, divulgado em 2018, dentre os ataques cibernéticos estão: sites com *malware* (1,7%); *phishing* de email (4%)[4]; *phishing* de premiação falsa (3%); *phishing* bancário (3,8%); *phishing* via app de mensagens (57,4%); notícias falsas (7%); golpes de SMS pago (3,1%); outros (0,9%). É um cenário preocupante (PSAFE, 2018). "63,8 milhões de ciberataques foram detectados somente no segundo trimestre do ano/2018. Isto significa que foram detectados 8 links maliciosos por segundo. Mais de 28 mil por hora." (PSAFE, 2018, n.p). Diante de um cenário preocupante - como regra de segurança da informação - o *compliance* digital tem atuado de forma incisiva com a função de realizar análise de riscos com o usode medidas preventivas como forma de garantir a adequação às novas regras da LGPD,com a proteção de dados.

Porém, há uma tecnologia disruptiva que tem atraído a atenção de várias empresas pelo mundo, por seu diferencial em proporcionar a imutabilidade, rastreabilidade, transparência e segurançados dados registrados – nomeada *Blockchain*.

Bilhões de dados registrados online são comprometidos por falhas de segurança. E a tecnologia *Blockchain* surge num momento importante da era digital, ao apresentar uma nova solução paraproporcionar segurança aos dados registrados online.

Segurança e Privacidade são dois pilares da LGPD, e a *Blockchain* é uma

[4] *Phishing*: é uma técnica de engenharia social usada para enganar usuários e obter informações confidenciais comonome de usuário, senha e detalhes do cartão de crédito. (NASCIMENTO, 2014).

ferramenta com potencial para atender à nova Lei geral de proteção de dados pessoais. Pois, a *Blockchain* já é uma realidade nas empresas de diferentes segmentos, sediadas em vários países e,também no Brasil, que identificam o valor em potencial da ferramenta.

Os contratos com novos modelos de negócios, que são programados na plataforma Ethereum, conhecida como *Smart Contracts* - os chamados Contratos Inteligentes autoexecutáveis, são exemplos de benefícios proporcionados pela *Blockchain*. Neste contexto, pode-se dizer que há uma tendência de o Direito e a Tecnologia caminharem juntos, com relação aos contratos programados.

O autor Andreas Sherborne (2017), cita um dos benefícios do *Smart Contract*, no manual do *International* BAR *Association,* intitulado "BLOCKCHAIN, SMART CONTRACTS AND LAWYERS":

> Os contratos inteligentes têm várias aplicações potenciais. Eles podem ser usados para transferir fundos de liquidação entre as partes mediante o cumprimento de uma obrigação definida, tais como uma aquisição corporativa ou compra de propriedade, ou para fazer o pagamento automático mediante a entrega de bens ou serviços. (SHERBONE, 2017, tradução nossa).

De acordo com o artigo 47 da LGPD, retromencionado, é obrigatória a garantia da segurança da informação dos dados. Mediante este contexto, nota-se que esta é uma estratégia à proteção de dados, desde que aliada a uma tecnologia que proporcione, além da segurança, transparência, imutabilidade, privacidade e rastreabilidade. Características presentes na nova tecnologia *Blockchain*.

Portanto, não existe proteção de dados sem segurança da informação; e sem segurança não existe privacidade; e sem privacidade não existe liberdade - garantias fundamentais na Constituição Federal de 1988.

3 COMO SURGIU A TECNOLOGIA *BLOCKCHAIN*

Blockchain é considerada uma ferramenta de registro, cujo significado da palavra é "cadeia deblocos" - local onde são registradas as transações e informações de dados.

Blockchain surgiu em 2008, junto com o Bitcoin, a partir da publicação de Satoshi Nakamoto, logo após a crise do subprime nos EUA, conhecida como a "bolha imobiliária americana", queatingiu a economia mundial. A partir de então, com o objetivo de acabar com a centralização do controle sobre o dinheiro, surgiu a primeira criptomoeda descentralizada, conhecida como Bitcoin - o marco na criação da criptoeconomia.

Em 2008, o misterioso Satoshi Nakamoto publicou um paper com a descrição técnica do *Blockchain* do Bitcoin, como solução para eliminar intermediários financeiros. No resumo inicial diz o seguinte: "uma versão puramente peer-to-peer de dinheiro eletrônico possibilita que pagamentos online sejam enviados diretamente de uma pessoa para a outra, sem precisar passar por uma instituição financeira." (FRANCO; BAZAN, 2018, p. 47).

As transações são registradas em cadeia de blocos, com o benefício de rastrear os gastos, evitar gasto duplo e, consequentemente, evitar alteração das informações. Por este motivo, *Blockchain* é conhecido como livro razão, porque em toda e qualquer transação financeira, as informações são computadas em um livro de registro, o que possibilita asegurança e a rastreabilidade das transações no *Blockchain* da bitcoin por meio da criptografia.

O livro razão registra todas as transações, sejam de débito e de crédito, de forma imutável, o que garante a integridade das informações, por serem invioláveis. Pode-se dizer que se trata deuma ferramenta com potencial à prevenção contra fraudes.

O surgimento do *Blockchain* da Bitcoin gerou uma revolução no mercado financeiro, com a mudança da concepção do uso da moeda física para a virtual, sem barreiras regulatóriase sem a necessidade de um intermediário – de um órgão financeiro, que são entidades centralizadorascom o poder econômico e político de controlar a circulação de moedas.

Um exemplo prático de uma das vantagens da rede descentralizada é que a transação, quando ocorre entre duas pessoas que não se conhecem, não precisa de um intermediário para validá-la. E, neste caso, não haverá a incidência de taxas pelos serviços que comumente são cobrados, quando há um intermediário financeiro.

Neste contexto, observa-se dois tipos de sistemas: um sistema controlado pelo governo(órgão central) e um sistema "distribuído" em que não cabe hierarquia, pois todos os participantes da rede descentralizada têm o poder de decisão, de escolha – perfazendo um poder compartilhadoentre os participantes da rede pública.

Com relação à criação do *Blockchain* de Bitcoin (BTC) em 2008, por Satoshi Nakamoto, pode- se dizer que outros autores também contribuíram para o surgimento das criptomoedas. A Forbes listou os 10 *whitepapers* mais importantes do mercado de criptomoedas publicados quase 30 anos antes do Bitcoin. Esses artigos científicos deram origem ao mercado de criptomoedas (JOSÉ, 2021)[5]. A seguir, estão descritos os estudos científicos, de forma cronológica.

Em 1979 foi o marco da "Assinatura digital certificada", através da publicação de Ralph C. Merkle, na qual descreve como as assinaturas digitais poderiam ser desenvolvidas, com o uso decriptografia; em 1991 é a vez de W.Scott Stornetta que descreve o princípio da inalterabilidadede dados, isto é, "Como registrar a data e hora de um documento digital" - *timestamp*; em 1994 é quando surgem os "Contratos Inteligentes", autoexecutáveis, publicado por Nick Szabo.

Já 2008 foi o marco da tecnologia *Blockchain*, descrita por Satoshi Nakamoto; em 2013 é o surgimento do *Ethereum*, com a geração de contratos inteligentes, publicado por Vitalik Buterin; em 2014 Dash Core Group, publica um modelo de privacidade de dados através da tecnologia *Blockchain*, chamado *Zerocash*, com a possibilidade de se efetuar pagamentos de forma anônima e descentralizada de *Bitcoin*; no mesmo ano, em 2014, Seigniorage desenvolvee apresenta como se obter a estabilidade na cotação da criptomoeda através de algorítimos;por fim, em 2020, Hayden Adams, Noah Zinsmeister e Dan Robinscon apresentam projetos definanças descentralizadas (DeFi). (JOSÉ, 2021).

[5] Contempla a lista dos 10 *white papers* mais importantes do mercado de criptomoedas.

4 TECNOLOGIA *BLOCKCHAIN* - ALIADA DA LGPD

Antes de adentrar no tema "Tecnologia *Blockchain*", é importante entender o que são dados pessoais, e elencar alguns artigos da nova Lei Geral de Proteção de Dados Pessoais, a LGPD, relacionados à segurança e privacidade desses dados. Pois, tanto a segurança quanto a privacidade são direitos fundamentais, garantidos pela Constituição Federal de 1988. De acordo com o Serviço Federal de Processamento de Dados – Serpro, é considerado Dado Pessoal:

> Se uma informação permite identificar, direta ou indiretamente, um indivíduo que esteja vivo, então ela é considerada um dado pessoal: nome, RG, CPF, gênero, data e local de nascimento, telefone, endereço residencial, localização via GPS, retrato em fotografia, prontuário de saúde, cartão bancário, renda, histórico de pagamentos, hábitos de consumo, preferências de lazer; endereço de IP (Protocolo da Internet) e cookies, entre outros. (SERPRO, 2022)

LGPD - Art. 5º. Para os fins desta Lei, define dado pessoal como informação relacionada à pessoa natural identificada ou identificável. Porquanto, o dado sensível está relacionadoà origem racial ou étnica, religião, opinião política, dado relacionado à saúde, opção sexual, e biometria. (BRASIL, 2018).

A sociedade vem se conscientizando que dado é um ativo pessoal e importante, devendoser resguardado com segurança e privacidade. Para que um cidadão conceda a terceiros (denominados "controladores"[6]), o seu direito de uso deverá obter, em contrapartida a garantiae o dever legal de preservá-los.

O dever legal é regido pela nova Lei Geral de Proteção de Dados Pessoais, a LGPD, definida como legislação brasileira que regula as atividades de tratamento de dados pessoais. De acordo com o Direito Fundamental à Proteção de Dados Pessoais em seu *Art. 17, "*Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e

[6] Lei no. 13.709/2018, LGPD – artigo 5º. VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

garantidos os direitos fundamentais de liberdade, intimidade e de privacidade, nos termos desta Lei".

A Privacidade é um Direito da personalidade, previsto no artigo 5º, inciso X, da CF 1988, a qual considera: "são inviol*áveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à* indeniz*ação pelo dano material ou moral decorrente de sua violaçã*o".É inquestionável a importância da segurança e privacidade dos dados pessoais. Portanto, as empresas que não desejam sofrer consequências jurídicas, com sanções administrativas aplicáveis pela autoridade nacional - previstas na nova Lei LGPD, no artigo 52 - estão se adequando à nova Lei Geral de Proteção de Dados Pessoais.

As empresas responsáveis pelo tratamento de dados pessoais, intitulados "controladores", devem exercer as atividades em restrito cumprimento à nova Lei LGPD tendo como enfoque, a segurança, citada em alguns artigos da Lei, tais como, descrito no artigo 6º. Inciso VII e no artigo 46º., respectivamente:

> Segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.
> [...]
> Agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

É notória a importância de que sejam implementadas soluções para garantir a privacidade durante todo o ciclo de vida dos dados tratados pelas empresas - "controladores". Mediante a citação de alguns artigos relacionados à nova Lei Geral de Proteção de Dados Pessoais, observa- se que a Segurança da Informação tem um papel importante em preservar esses dados, aliada àtecnologia de ponta para atender as demandas legais e comerciais.

Dentre as tecnologias apontadas, a *Blockchain*, conhecida como "protocolo de confiança", é umaferramenta que tem aguçado a curiosidade do setor privado e setor

público, por proporcionar segurança, assegurar a privacidade e integridade dos dados. *Blockchain* é uma ferramenta de registro que tem proporcionado segurança no mundo online, sem burocracia e com custo reduzido para sua implementação. Dentre seus benefícios: evita alteração de informações, gasto duplo nas transações, mitiga riscos de fraudes - dentre outros benefícios - devido as suas características de imutabilidade, rastreabilidade e integridade dos dados, com segurança.

5 *BLOCKCHAIN* E SEUS BENEFÍCIOS

Blockchain é conhecido como "livro razão", por ser uma ferramenta onde se registra qualquer informação e/ou transações financeiras, de forma compartilhada e distribuída em redes descentralizadas. É um meio de se registrar qualquer tipo de documento com fins de garantir a integridade desse registro de forma segura. Por esse motivo, é considerado um sistema confiável devido as suas características de inviolabilidade, imutabilidade e transparência.

Blockchain foi criado para que o primeiro sistema financeiro do Bitcoin funcionasse. E, desde então, a ferramenta tem sido explorada para diferentes fins. Por exemplo, na plataforma, pode-se programar qualquer aplicativo para atender a diferentes demandas. Desde transação de moedas digitais, registros de todo tipo de dados e documentos, até a programação de contratos inteligentes autoexecutáveis. A segurança proporcionada pela ferramenta *Blockchain* conta com o uso de diferentes tecnologias, tais como: a criptografia, função *hash*, cerificados digitaise assinatura digital e P2P- rede ponto a ponto.

A criptografia é que garante a segurança, pois, seu funcionamento se dá com base em cálculos matemáticos que transformam uma mensagem em uma sequência de caracteres (TEIXEIRA; RODRIGUES, 2021, p. 25). O *hash* é um algoritmo que tem a função de encadear as informações de forma a garantir a integridade dos dados.

O P2P é uma rede ponto a ponto que quebra o conceito de rede centralizada. Neste caso, todos os nós de uma rede possuem uma cópia idêntica da base de dados,

possibilitando o compartilhamento simultâneo a todos os usuários da rede descentralizada. Trata-se de uma rede de testemunha para todas as transações. Por esse motivo, todos têm a cópia de todos os registros.

Como mencionado anteriormente, *a Blockchain* do Bitcoin foi criada para eliminar intermediários financeiros. Por esse motivo é considerada uma rede descentralizada por não precisar de um terceiro porque as transações são validadas por mineradores, que são as testemunhas da própria rede. Esses validadores seguem as regras estabelecidas, o que faz com que a rede se torne confiável, sendo conhecida como o "Protocolo da Confiança", segundo Don Tapscott e Alex Tapscott (2016).

Blockchain é conhecido como protocolo de confiança por atribuir segurança às transações realizadas com as criptomoedas. Portanto, quando ocorrem as transações, não se associam à identidade do usuário, devido ao uso de chaves criptográficas para que se possa realizar as transações de forma segura.

Trata-se de duas chaves, a chave pública (em que todos os participantes da rede têm acesso)e a chave privada (somente o detentor da criptomoeda tem acesso). A chave pública é para gerar um endereço público para as transações serem efetivadas – como se fosse informações deagência e conta corrente (FRANCO; BAZAN, 2018, p. 106). A *Blockchain* é uma ferramenta pública ou aberta, que faz registro de informações auditáveis e rastreáveis, distribuídas por uma rede não centralizada, com toda transparência da informação. Rede esta que possibilita que qualquer pessoa se conecte a ela. A *Blockchain* usa um algoritmo de consenso, conhecido como "*Proof-of-work*" que determinacomo novos blocos serão adicionados.

Existem, também, as *Blockchains* fechadas ou privadas que são aqueles em que apenas participantes pré-selecionados podem participar da rede, sendo conhecidas como rede DTL – *Distributed Ledger Technology* (Tecnologia de Registro Contábil Distribuído).

Blockchain é uma tecnologia utilizada em diferentes setores do mercado, com fins variados, desde setores financeiro, social, *supply chain*, até o setor público. O seu diferencial vem contribuindo também, no setor jurídico, quando se trata de serviços

cartorários, de propriedade intelectual – registro de autoria de obras, marcas e patentes, de *cyber*segurança, em licitações enas relações contratuais, com a introdução dos Contratos Inteligentes.

Dentre os diversos benefícios - com o registro das informações em blocos - pode-se destacar oregistro de provas digitais, utilizadas em processos judiciais. "*O Blockchain e suas aplicações extrapolam o âmbito financeiro e podem ser usados como solução para inúmeros problemas defraude, adulteração e falsificação que existem hoje na sociedade"*. (FRANCO; BAZAN, 2018, p. 104-5)

Um dos benefícios da *Blockchain,* além da segurança, é a de proporcionar a privacidade no ambiente digital através da criptografia - o que faz *Blockchain* ser visto como um diferencial tecnológico que vai ao encontro de exigências impostas pela LGPD, Marco Civil da Internet, Código Civil e a Constituição Federal de 1988. A LGPD, trata de Privacidade em seu art. 2º, ao dispor sobre a "*disciplina da proteção de dados pessoais tem como fundamentos: I - o respeito à privacidade"* (BRASIL,2018).

Por conseguinte, o Marco Civil da Internet (MCI) - Lei nº 12.965 de 23 de Abril de 2014, considera como Privacidade, em seu artigo 8º. – "A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acessoà internet" (BRASIL, 2014). No Decreto nº 8.771/2016, que regulamenta o Marco Civil da Internet, trata de Segurança (BRASIL, 2016) em seu art. 13: "Os provedores de conexão e de aplicações devem, na guarda, armazenamento e tratamento de dados pessoais e comunicações privadas, observar as seguintes diretrizes sobre padrões de segurança".

O Código Civil, no artigo 21, considera a Privacidade "A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma" (BRASIL, 2002). A Constituição Federal (CF) de 1988 prevê em seu artigo 5º, inciso X, que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação" (BRASIL, 1988).

Como se pode observar, a tecnologia Blockchain tem várias funcionalidades, sendo, portanto, motivo para atrair o interesse de várias empresas. Por conseguinte, vários países já adotam a tecnologia Blokchain, como exemplo:

> Na Holanda, algumas cidades criaram aplicativos desenvolvidos em Blockchain para administrar contratos imobiliários, enquanto nos Estados Unidos, o serviço postal trabalha com Blockchain desenvolvendo uma ferramenta para monitorar suas entregas. (CHAGAS, 2019)

6 *SMART CONTRACT* – O NOVO MODELO DE NEGÓCIO JURÍDICO

O *Smart Contract*, na sua tradução literal "Contratos Inteligentes", é um contrato traduzido em linguagem de programa conhecido como *Solidity*. Isto é, são contratos programados para serem autoexecutáveis.

O Contrato Inteligente surgiu em 1994 através de Nick Szabo, ao publicar a descrição do projeto através do *whitepaper*, na revista *Extropy*, com a proposta da programação de contratos autoexecutáveis. Szabo, afirma que: "Um contrato inteligente *é um protocolo de transação computadorizado que executa os termos de um contrato"* (SZABO, 1994, tradução nossa).[7] Nick Szabo é jurista e criptógrafo, responsável por introduzir o conceito inovador sobre contratos digitais por sua praticidade no manuseio dos contratos em projetos que envolvam comércio eletrônico.

De acordo com o site da Ethereum, "um contrato inteligente é um conjunto de regras registradas em cadeias de blocos de informações para que todos vejam e executem exatamente de acordo com essas regras." (ETHEREUM, 2022, tradução nossa).[8]

Já em 2013 foi o marco do surgimento da *Ethereum*, que foi apresentado como plataforma para o desenvolvimento de projetos descentralizados, através da publicação do *whitepaper*, escrito porVitalik Buterin. A *Ethereum* é uma plataforma pública e de

[7] No original: "*A smart contract is a computerized transaction protocol that executes the terms of a contract*". (SZABO, 1994).
[8] No original: "*A smart contract is like a set of rules that live on-chain for all to see and run exactly according to those rules*". (ETHEREUM, 2022).

código aberto para o desenvolvimento de projetos descentralizados, onde são escritos os contratos em linguagem de programação. Como definição, pode-se dizer que o Ethereum é: "uma plataforma descentralizada focada na execução dos chamados 'contratos inteligentes', operações que são feitas automaticamente quando certas condições são cumpridas" (INFOMONEY, 2021). Em suas operações, utiliza a sua própria moeda, o Ether, e, também, de outros ativos. Ethereum, por outro lado, é um protocolo construído em blockchain com o propósito de executar smart contracts, os contratos digitais programáveis.

Durante a XVIII Reunião Plenária da Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro, que ocorreu em dezembro de 2020, em Brasília/DF, com a participação de órgãos púbicos, "Contrato Inteligente" foi citado com a seguinte definição: "são códigos-fonte em linguagem de programação (scripts), que podem ser definidos e auto executados em uma infraestrutura de blockchain." (TCU, 2020).

Portanto, a junção da tecnologia *Blockchain* do *Bitcoin* com o conceito de Contratos Inteligentes, proporcionou o desenvolvimento dos Contratos Inteligentes na plataforma *Blockchain* do *Ethereum*, onde são efetivadas as transações financeiras descentralizadas (DeFi) dos contratos inteligentes.

> *Blockchain* tem possibilitado a criação de contratos inteligentes. Contratos inteligentes são essencialmente implementados na plataforma de *blockchains*. As cláusulas contratuais aprovadas são convertidas em programas de computador executáveis. As conexões lógicas entre as cláusulas contratuais são preservadas de acordo com os fluxos lógicos da programação. A execução de cada contrato é registrada de forma imutável e armazenada no *blockchain.* Contratos inteligentes garantem o adequado controle de acesso e a execução de contrato. (ZHENG *et. all*, 2020, tradução nossa).

A finalidade dos Contratos Inteligentes é de proporcionar celeridade e efetividade do serviço prestado, de forma automática, com a garantia do pagamento, sem a necessidade de um intermediário. Evitando, dessa forma, custos de transação, o que, consequentemente, possibilitaa criação de novos modelos de negócio.

Um dos diferenciais da tecnologia são as suas características de imutabilidade, rastreabilidade e segurança. Sendo assim os registros não podem ser apagados, podendo ser auditáveis, com toda segurança proporcionada pela tecnologia. Um outro diferencial é a descentralização das informações, isto é: "(…) quando contratos inteligentes são implementados em um blockchain, sua execução n*ão ser*á *executada em um servidor central, mas sim distribuída entre a rede de nós*." (TEIXEIRA; RODRIGUES, 2021, destaques nossos).

No portal do Tribunal de Contas da União, consta a definição sobre como funciona o Contrato Inteligente, isto é, como sendo um contrato executado pelos nós e os resultados da execução são validados por consenso e registrados no livro-razão distribuído. Ressalta, também, que sua automação reduz custos e riscos de erros, além de mitigar riscos de fraude e otimizar processos de negócios (BRASIL, 2022). Embora, ainda não haja regulamentação no Brasil, a utilização de contratos inteligentes provê as seguintes vantagens:

> **transparência**: contratos inteligentes podem ser escritos e verificados a qualquer momento por todas as partes envolvidas, que podem verificar podem verificar o código-fonte do contrato;
> **menor prazo para execução**: a eliminação dos passos manuais torna a execução do contrato mais rápida e eficiente;
> **precisão**: como o contrato é descrito por um algoritmo computacional, sua execução é precisa, salvo se houver erro de programação;
> **segurança**: a infraestrutura de DLT garante a segurança em contratos inteligentes, que são assinados por chaves criptográficas e não podem ser violados por terceiros sem permissão de acesso;
> **rastreabilidade**: os dados de cada execução das "funções" do contrato ficam armazenados na DLT, permitindo que a execução do contrato seja auditável a qualquer tempo;
> **menor custo**: por sua natureza digital e em razão da eliminação de intermediários, os contratos inteligentes reduzem os custos de execução;
> **confiança**: as características citadas acima levam à maior confiança entre as partes envolvidas no contrato. (TCU, 2020)

O Brasil tem discutido sobre o tema e, aos poucos, aderindo à tecnologia. Por exemplo, a Comissão de Valores Mobiliários (CVM), publicou em setembro de 2018, o

Ofício Circular n.1/2018/CVM/SIN, no qual permite o investimento em criptoativos de forma indireta pelos fundos de investimentos brasileiros (GLASMEYER, 2021).

> A Receita Federal brasileira publicou em maio de 2019 a Instrução Normativa 1888 (IN 1.888) que traz uma série de definições importantes, incluindo a definição legal de criptoativos na jurisdição brasileira: o criptoativo é a a representação digital de valor denominada em sua própria unidade de conta, cujo preço pode ser expresso em moeda soberana local ou estrangeira, transacionado eletronicamente com a utilização de criptografia e de tecnologias de registros distribuídos, que pode ser utilizado como forma de investimento, instrumento de transferência de valores ou acesso a serviços,e que não constitui moeda de curso legal. (GLASMEYER, 2021, n.p).
> No Brasil não existe regulamentação deste tipo de contrato, ocorre que, não havendo legislação específica, estes contratos são caracterizados como atípicos, devendo para atendê-los ser utilizado o artigo 425 da Lei nº 10.406 de 10 de janeiro de 2002 (Código Civil): "É lícito às partes estipular contratos atípicos,observadas as normas gerais fixadas neste Código" (BRASIL, 2022).

Dentre os benefícios da prestação de serviços programados via *blockchain*, além de evitar alteração contratual, também, evita a judicialização e o inadimplemento, pois, de acordo com as evidências coletadas pelo uso da tecnologia em um determinado contrato de prestação de serviço, por exemplo, empreiteira:

> O pagamento só seria liberado para a empreiteira após a entrega completa do projeto. Como os pagamentos seriam gerenciados pelo contrato inteligente e registrados no *blockchain*, o desvio de verba se tornaria impossível (FRANCO; BAZAN, 2018, p. 104).

Um outro fator benéfico é que evita a ocorrência de fraudes contratuais pelo fato da topologia do *Blockchain* ser descentralizada, de acordo com a explicação do Tribunal de Contas da União que fez um levantamento sobre o potencial da tecnologia, em 2020, como diz a seguir:

> A descentralização é uma característica do blockchain, por não ter um servidor central único, e sim um servidor distribuído em vários pontos do mundo, conhecido como "os mineradores" sendo, portanto, um diferencial com fins de evitar ataques de hackers. Isto é, as informações não ficam centralizadas em um único local, mas distribuídas entre os mineradores - quem validam as transações. Trata-se de um sistema democrático devido a descentralização do poder da informação.

> O gerenciamento de dinheiro público é uma área em que soluções *blockchain* podem ajudar a minimizar fraudes e aumentar a transparência e responsabilidade dos entes envolvidos. Por exemplo, com a utilização de contratos inteligentes, é possível estabelecer que repasses de determinado programa de governo sejam efetivamente realizados somente se a transação for legítima, considerando parâmetros como valor, beneficiários, temporalidade, área de aplicação do recurso, entre outros (BRASIL, 2020).

Estudar Contratos Inteligentes pode ser considerado o meio para se apontar questionamentos mais relevantes a respeito dos modelos de contratos, de forma a compreendê-los e assimilar seus benefícios para serem adotados nas organizações.

Os Contratos Inteligentes têm possibilitado a adoção de novos modelos de negócio na esfera empresarial, por meio de automação de contratos programados através de código-fonte, graças as tecnologias adotadas na plataforma *Blockchain*, com o uso da criptografia, assinatura digital, da função *hash* e P2P (rede ponto a ponto).

A era digital já é uma realidade e os profissionais da área jurídica no Brasil tendem a se adequar a esta nova demanda, por se tratar de gestão contratual. As discussões sobre o tema são necessárias e pertinentes, uma vez que não se pode discutir subjetividades em contratos autoexecutáveis.

> As diferenças cruciais entre os contratos tradicionais e os contratos inteligentes são que a lógica da lei tradicional é baseada na interpretação «subjetiva» da analogia, de acordo com Szabo. Por outro lado, os contratos inteligentes de *blockchain* são baseados em «bits e lógica» booleanos que sustentam o Bitcoin. (CASTILLO, 2021, tradução nossa).[9]

Por fim, a tecnologia *Blockchain* tem sido adotada devido as suas inúmeras possibilidades, seja em processo de compra e vendas, licitações, registro de dados de saúde, transferência de ativos, *supply chain*, dentre outros, sendo também, capaz de combater fraudes. Trata-se de uma ferramenta estratégica, seja para empresas privadas, como, também, para empresas públicas.

[9] No original: "*Crucial differences between traditional contracts and smart contracts are that the logic in traditional law is based on the "subjective" interpretation of analogy, according to Szabo. On the other hand, blockchain smart contracts are based on Boolean "bits and logic" that underpin bitcoin*".

7 BLOCKCHAIN NO DIREITO BRASILEIRO

A tecnologia Blockchain tem demonstrado seu valor em diferentes setores do mercado, seja privado ou público, e quanto as suas implicações jurídicas destaca-se a apresentação de provas judiciais, com respaldo no artigo 369 do Novo Códido de Processo Civl: "As partes têm o direito de empregar todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código, para provar a verdade dos fatos em que se funda o pedido ou a defesa e influir eficazmente na convicção do juiz" (BRASIL,2015). No judiciário o reconhecimento de provas já é uma realidade, embora de forma incipiente.

> O Tribunal de Justiça de São Paulo, ao julgar o Agravo de Instrumento nº 2237253- 77.2018.8.26.0000, ainda em dezembro de 2018, entendeu ser desnecessária a concessão de tutela para abstenção de comunicação de terceiros a respeito do pedido formulado na ação (fornecimento de dados de usuários responsáveis por publicações ofensivas no Facebook e Twitter), uma vez que o conteúdo tido como violador dos direitos do autor da ação já havia sido preservado via *blockchain*. A 5ª Câmara do TJ-SP entendeu, então, que tal preservação seria hábil a comprovar a veracidade e existência do conteúdo, chancelando a validade da prova registrada em *blockchain* (BRASIL, 2021; BRAGUIN; VAZQUEZ, 2021).

Dentre as diversas finalidades de uso da *Blockchain*, pode-se citar:

> O armazenamento em *blockchain*, por exemplo, é utilizado em plataformas de financiamento eleitoral homologadas pelo TSE para as eleições (...). A Federação Brasileira dos Bancos (Febraban), por sua vez, tem desenvolvido um sistema de armazenamento de dados em *blockchain* que compartilha, de forma criptografada, informações de dispositivos móveis, como *smartphones* e *tablets*, usados em transações bancárias, o que permitiria que eventual comunicação de furto ou roubo do aparelho seja compartilhada entre todas as instituições financeiras. (ROQUE, 2018, n.p).

O campo da Propriedade Intelectual, também, pode se beneficiar com a aplicação desta tecnologia, com o objetivo de comprovar a autenticidade autoral, uma vez que a

tecnologia dispõe do recurso de *timestamp* ou carimbo do tempo que é uma cadeia de caracteres que registra a hora ou data em que certo evento ocorreu.[10]

Segundo a Organização Mundial da Propriedade Intelectual (WIPO),

> A adoção da tecnologia de *blockchain* na gestão de direitos de PI exigiria um conjunto de normas acordadas e internacionalmente apoiadas. Será importante que as autoridades reguladoras e os elaboradores de políticas públicas trabalhem juntos para ajudar a realizar a implementação desta tecnologia no âmbito do registro dos direitos de PI. (ROSE, 2020).

O serviço de Registro de Imóveis, também, já se beneficia da tecnologia. Recentemente, a Corregedoria-Geral da Justiça regulamentou "a lavratura de escrituras públicas de permuta de bens imóveis com contrapartida de *tokens*/criptoativos e o respectivo registro imobiliário pelos Serviços Notariais e de Registro do Rio Grande do Sul", através do Provimento nº 038/2021 (TJRS, 2021).

Por outro lado, o Governo Brasileiro já vem estudando e desenvolvendo projetos com o uso da tecnologia *Blockchain*, tais como: RNDS - Registros Eletrônicos de Saúde, em *Blockchain*; TRUBUDGET – sistema de monitoramento de doação de recursos com acompanhamento dos gastos à prestação de contas; bConnect – ferramenta de colaboração para troca de dados entre países do Mercosul; BCPF E BCNPJ – Receita Federal – é uma rede permissionada do *blockchain* como meio de compartilhamento de dados. bCPF e bCNPJ são dois projetos com objetivo de viabilizar a colaboração sobre a base de dados do Cadastro de Pessoas Físicas (CPF) e Jurídicas (CNPJ); PIER - Plataforma de Integração de Informações das Entidades Reguladoras. Ferramenta de registro da interação entre instituições financeiras e órgãos regulatórios; SISTEMA DE CONTRATOS DISTRIBUÍDOS - Compartilhamento de informações padronizadas sobre processos públicos de compra; BNDESTOKEN - Serviços de financiamentos do BNDES (TCU, 2020).

[10] "Um carimbo do tempo (CT) é um documento eletrônico que serve para atestar a data e hora que um documento existia ou que uma transação digital foi realizada" (VIVIAN, 2018).

8 CONSIDERAÇÕES FINAIS

A pesquisa realizada apresenta os fundamentos da introdução de uma nova tecnologia disruptiva, a *Blockchain*, e seus benefícios no mundo corporativo, em empresas privadas e públicas.

A análise atestou a existência de uma tecnologia que vem impactando positivamente o mercado. Dentre seus benefícios, pode-se citar o de atender certas exigências da Lei Geral de Proteção de Dados Pessoais – LGPD no que tange à privacidade, transparência e segurança. Sua adoção enseja inúmeras possibilidades de introdução de novos modelos de negócios, num mundo que está caminhando para o digital.

Não se trata de uma tecnologia incipiente, conforme se demonstrou sua aplicabilidade em diferentes segmentos de mercado. Portanto, requer dos advogados um novo perfil profissional com visão multidisciplinar e tecnológica para auxiliá-los nesta nova demanda de mercado.

Os benefícios no mundo jurídico foram relatados de forma exemplificativa, pois a tecnologia referida abre um leque de possibilidades para atender ao mercado que tem se apresentado cada vez mais exigente - sejam empresas do setor privado ou público. O seu potencial é vasto, e tem provocado mudanças em vários setores, principalmente, no setor financeiro. A pesquisa, aqui apresentada, é apenas o meio para que se possa dar continuidade ao assunto de extrema importância no mundo jurídico, sobre a Regulamentação das criptomoedas, inseridas nos novos modelos de negócio. Inclusive, já tramita na Câmara Federal o projeto PLC 2.303/2015 com a inclusão de moedas digitais e PLC 2.060/2019, que reconhece a licitude da emissão e circulação de criptomoedas e criptotokens por pessoas jurídicas, (TEIXEIRA; RODRIGUES, 2021, p.83), além de dois projetos que foram apresentados no Senado Brasileiro com foco na regulação das criptomoedas e corretoras (PLS 3.825/2019 e PLS 3.849/2019).

Neste contexto, os órgãos reguladores terão pela frente um papel importante com

relação às regras de transações com criptomoedas e suas tributações. É um assunto vasto, que envolve a nova economia digital em âmbito mundial, com fins tributáveis. Assunto, este, já sendo liderado pela Organização para a Cooperação e Desenvolvimento Econômico – OCDE[11], podendo, inclusive, ser assunto para um próximo artigo.

Como conclusão da pesquisa, observou-se que, a introdução de novas tecnologias tem sido aderida pela sociedade e, consequentemente, tem modificado o seu comportamento e a maneira de fazer negócios. Sendo assim, mediante a mudança do perfil da sociedade, é notória a necessidade do sistema jurídico se alinhar a essa nova realidade, pois a mudança cultural da sociedade, através da transformação digital, tem impactado a forma de produzir e trabalhar, e os advogados precisam estar preparados para atender a essa nova demanda.

REFERÊNCIAS

BRAGUIN; VAZQUEZ, 2021. **A validade da prova registrada em blockchain no judiciário**. Disponível em: www.conjur.com.br/2021-mar-11/braguim-vazquez-validade-prova-registrada-blockchain. Acesso em: 05 dez 2022.

BRASIL, Norma Brasileira, NBR. **ABNT NBR ISO/IEC 27002 de outubro de 2022**. Disponível em: https://www.normas.com.br/visualizar/abnt-nbr-nm/21529/nbriso-iec27002-seguranca-da-informacao-seguranca-cibernetica-e-protecao-a-privacidade-controles-de-seguranca-da-informacao. Acesso em: 04 abr. 2023

BRASIL, Presidência da República. **Constituição da República Federativa de 1988**. Disponível em: www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: dez. 2021

BRASIL, Presidência da República. **Decreto nº 8.771/2016, de 11 de maio de 2016.** Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego(...). Disponível em: www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm. Acesso em: dez 2021

[11] OCDE aborda sobre a política tributária no contexto da moeda virtual, em seu relatório de 14 out.2020, *Taxing Virtual Currencies: An Overview of Tax Treatments and Emerging Tax Policy Issues*.

BRASIL, Presidência da República. **Lei no. 10.406 de 10 de janeiro de 2002** (Código Civil). Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 15 dez 2022.

BRASIL, Presidência da República. **Lei nº13.105, de 16 de março de 2015. Código de Processo Civil**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 15 dez. 2022.

BRASIL, Presidência da República. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: dez 2021

BRASIL, Presidência da República**. Lei nº 12.965, de 23 de abril de 2014**. Marco Civil da Internet. Disponível em: www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: dez 2021

BRASIL. Presidência da República. Controladoria Geral da União, **CGU** . **Portal da Transparência** – Disponível em: www.gov.br/cgu. Acesso em: set. 2022.

BRASIL, Presidência da República. Ministério da Fazenda. **O que são dados pessoais, segundo a LGPD**. Disponível em: www.serpro.gov.br/lgpd/menu/protecao- de-dados/dados-pessoais-lgpd. Acesso em:14 nov 22.

BRASIL, Presidência da República. Ministério da Justiça e Segurança Pública. ENCCLA – ***Blockchain* e o Setor Público no Brasil**. Youtube disponível em: www.youtube.com/watch?v=NFn0Np_nEEk. Setembro, 2020. Acesso em: out. 2021.

BRASIL. Presidência da República. Tribunal de Contas da União, TCU. **Levantamento da Tecnologia Blockchain. 2020**. Disponível em: https://portal.tcu.gov.br/levantamento-da-tecnologia-blockchain.htm. Acesso em: 30 set. 2022.

BRASIL. Rio Grande do Sul. Tribunal de Justiça do Rio Grande do Sul, TJRS**. CGJ regulamenta escritura pública de imóveis por token/criptoativo**. Disponível em: www.tjrs.jus.br/static/2021/11/Provimento-038-2021-CGJ.pdf. Acesso em: 13 dez 2022.

CASTILHO, Michael de. Smart contract inventor Nick Szabo has said lawyers' roles are "complimentary" to the role of smart contracts. **Coindesk,** 8/12/2016. Disponível em: www.coindesk.com/markets/2016/12/08/relax-lawyers-nick-szabo-says-smart-contracts-wont-kill-jobs/. Acesso em: 30 out. 2022.

CHAGAS, Edgar. **Blockchain: a revolução tecnológica e impactos para a economia**. Disponível em: www.nucleodoconhecimento.com.br/tecnologia/blockchain. Acesso em: 04 abr. 2023.

DONDA, Daniel. **Guia Prático de Implementação da LGPD**. São Paulo: Labrador Forense, 2020.

ETHEREUM. Disponível em: https://ethereum.org/en/dapps/. Acesso em: 30 out. 2022.

FRANCO, A.; BAZAN, V. **Cripto Moedas: Melhor que Dinheiro**. Ed. Empiricus, 2018, p. 104 São Paulo, 2018.

GLASMEYER, Rodrigo. **Regulação das criptomoedas no Brasil e no mundo**. São Paulo, 2021. Disponível em: https://blconsultoriadigital.com.br/regulacao-das-criptomoedas/. Acesso em: 30 set. 2022.

IBIJUS, Instituto Brasileiro de Direito. **Contratos Inteligentes**. Disponível em: www.ibijus.com/blog/580-consideracoes-sobre- a-aplicacao-dos-contratos-inteligentes-no-brasil. Acesso em: 30 set. 2022.

INFOMONEY. **Ethereum**. Disponível em: www.infomoney.com.br/cotacoes/ethereum-eth/. Acesso em: 30 out. 2021

JOSÉ, Paulo. **Forbes lista os 10 white papers mais importantes do mercado de criptomoedas**. Disponível em: https://br.cointelegraph.com/news/forbes-lists-the-10-most-important-white-papers-in-the-cryptocurrency-market. Acesso em: 04 abr. 2023.

NASCIMENTO, Anderson. O que é *phishing*. **CanalTech**, 02/07/2014. Disponível em: https://canaltech.com.br/seguranca/o-que-e-phishing/. Acesso em: dez.2021.

Norma **ISO 27002**, 2022. Disponível em: https://www.normas.com.br/visualizar/abnt-nbr-nm/21529/nbriso-iec27002-seguranca-da-informacao-seguranca-cibernetica-e-protecao-a-privacidade-controles-de-seguranca-da-informacao. Acesso em: 04 abr. 2023

OCDE, Organização para a Cooperação e Desenvolvimento Econômico. ***Taxing Virtual Currencies****: An Overview of Tax Treatments and Emerging Tax Policy Issues.* Disponível em:www.oecd.org/tax/tax-policy/flyer-taxing-virtual-currencies-an-overview-of-tax-treatments-and-emerging-tax-policy-issues.pdf . Acesso em: 22 out 2021

POYATOS, Henrique. ***Blockchain Advanced*.** Disponível em: ://on.fiap.com.br/. Pdf. Acesso em: nov.2021.

PSAFE, DFNDR. **Relatório de Segurança Digital no Brasil**. Disponível em: https://www.psafe.com/dfndr-lab/wp-content/uploads/2018/08/dfndr-lab-Relat%C3%B3rio-da-Seguran%C3%A7a-Digital-no-Brasil-2%C2%BA-trimestre-de-2018.pdf. Acesso em: 04 abr. 2023.

RANSOMWARE: definição, prevenção e remoção. Disponível em: www.kaspersky.com.br/resource-center/threats/ransomware. Acesso em: dez.2021.

ROQUE, André Vasconcelos. **A tecnologia blockchain como fonte de prova no processo civil**. Acesso em, v. 23, 2018. Disponível em: https://ab2l.org.br/a-tecnologia-blockchain-como-fontede-prova-no-processo-civil/. Acesso em: 30 abr. 2023.

ROSE, Anne. **Blockchain: transformando o registro de direitos de PI e fortalecendo a proteção dos direitos de PI não registrada**. Disponível em: www.wipo.int/wipo_magazine_digital/pt/2020/article_0002.html Acesso em: 5 dez.2021.

SHERBONE, A., ***Blockchain, Smart Contracts and Lawyers***. BAR International Association, Dec 2017. Disponível em: https://theblockchaintest.com/uploads/resources/International%20Bar%20Association%20-%20Blockchain%20smart%20contracts%20and%20lawyers%20-%202017%20-%20Dec.pdf. Acesso em: nov.2021

SZABO, Nick. **Contratos Inteligentes**. Wikipédia enciclopédia. Disponível em: https://pt.wikipedia.org/wiki/Nick_Szabo. Acesso em: 30 set. 2022.

SZABO, Nick. ***Smart Contracts***. Disponível em: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html. 1994. Acesso em: 04 out. 2022.

TAPSCOTT, Don; TAPSCOTT, Alex. ***Blockchain Revolution*: Como a tecnologia por trás do Bitcoin está mudando o dinheiro, os negócios e o mundo**. São Paulo: SENAI Forense, 2016.

TEIXEIRA, Tarcísio; RODRIGUES, Carlos Alexandre. ***Blockchain* e Criptomoedas, aspectos jurídicos**, 2. ed. Salvador: JusPodivm Forense, 2021.

THE AME GROUP. ***Data Security Breach: 5 Consequences for Your Business***. Disponível em: https://www.theamegroup.com/security-breach/. Acesso em: 04 abr. 2023.

VIVIAN, Darlan. **Carimbo do tempo, na overviewzheng e protocolo digital**: entenda as diferenças. BRySigner, 24/08/2018. Disponível em: https://www.bry.com.br/blog/carimbo-do-tempo-timestamp/. Acesso em 30 abr. 2023.

ZHENG, Zibin *et al*. An overview on smart contracts: Challenges, advances and platforms. **Future Generation Computer Systems**, v. 105, p. 475-491, 2020.

A LIBERDADE DIGITAL NA SOCIEDADE DE RISCO: PERSPECTIVAS A PARTIR DA PROTEÇÃO DE DADOS PESSOAIS

DIGITAL FREEDOM IN THE RISK SOCIETY: PERSPECTIVES BASED ON PERSONAL DATA PROTECTION

Pedro Henrique Hermes[1]

Rogério Gesta Leal[2]

RESUMO: O presente trabalho tem o seguinte problema de pesquisa: como o direito fundamental à liberdade no ambiente digital pode ser protegido pelo direito fundamental à proteção de dados pessoais e a Lei nº. 13.708/18 (Lei Geral de Proteção de Dados Pessoais)? Utilizou-se, para responder ao questionamento, o método de abordagem dedutivo e método de procedimento o monográfico. Como resultado, constatou-se que a proteção de dados pessoais é importante baliza na discussão entre sobre liberdade na Internet, especialmente a liberdade digital. Com isso, a regulação dos dados pessoais no Brasil constitui o ponto de equilíbrio em face das relações multifacetadas que envolvem o tema.

Palavras-chave: liberdade digital; proteção de dados pessoais; Sociedade de Risco.

---

[1] Doutorando em Direito na Universidade de Santa Cruz do Sul (UNISC), na linha de pesquisa Dimensões Instrumentais das Políticas Públicas - Bolsa Prosuc CAPES II. Mestre em Direito na Universidade de Santa Cruz do Sul (UNISC), na linha de pesquisa Constitucionalismo Contemporâneo - Bolsa Prosuc CAPES II. Graduado em Direito pela Antonio Meneghetti Faculdade (AMF). Professor de graduação no curso de Direito da Antonio Meneghetti Faculdade (AMF). Coordenador do Laboratório de Inovação e Direito da Antonio Meneghetti Faculdade (AMF). Advogado. Lattes: http://lattes.cnpq.br/1086414991223763.

[2] Possui graduação em Direito pela Universidade de Santa Cruz do Sul (1987), mestrado em Desenvolvimento Regional pela Universidade de Santa Cruz do Sul (1997); doutorado em Direito pela Universidade Federal de Santa Catarina (2000) e doutorado na Universidad Nacional de Buenos Aires(2004). Atualmente é professor titular da Universidade de Santa Cruz do Sul. e da Fundação Escola Superior do Ministério Público do Rio Grande do Sul - FMP, nos cursos de graduação, mestrado e doutorado em direito. Tem experiência na área de Direito, com ênfase em Direito Administrativo, Direito Penal e Processual Penal, atuando principalmente nos seguintes temas: Estado, Administração Pública e Sociedade. Enfrentamento da corrupção pelo Direito Penal e Processual Penal. Sociedade de Riscos. Lattes: http://lattes.cnpq.br/7185339028226710.

ABSTRACT: The present work has the following research problem: how the fundamental right to freedom in the digital environment can be protected by the fundamental right to the protection of personal data and Law nº. 13.708/18 (General Personal Data Protection Law)? The deductive method of approach and the monographic method of procedure were used to answer the question. As a result, it was found that the protection of personal data is an important guideline in the discussion about freedom on the Internet, especially digital freedom. With this, the regulation of personal data in Brazil constitutes the balance point in the face of the multifaceted relationships that involve the subject.

Keywords: digital freedom; protection of personal data; Risk Society.

1 INTRODUÇÃO

A tecnologia digital avançou rapidamente nas últimas décadas, possibilitando uma ampliação significativa da troca de informações e interações sociais. Entretanto, essa mesma evolução trouxe novos desafios jurídicos, especialmente no que diz respeito à liberdade digital e proteção de dados pessoais.

O objetivo deste artigo científico é analisar os impactos da evolução tecnológica sobre os direitos de liberdade digital e proteção de dados pessoais. Para tanto, será utilizada a metodologia de revisão bibliográfica, com o objetivo de identificar a problemática central da pesquisa e levantar as principais contribuições teóricas e práticas sobre o tema.

O problema de pesquisa a ser abordado é a necessidade de encontrar um equilíbrio entre o direito à liberdade digital e a proteção de dados pessoais, considerando a complexidade das relações sociais e econômicas em ambientes digitais. Parte-se do seguinte questionamento e problemática: como o direito fundamental à liberdade no ambiente digital pode ser protegido pelo direito fundamental à proteção de dados pessoais e a Lei nº. 13.709/18 (Lei Geral de Proteção de Dados Pessoais)? O objetivo principal é propor reflexões críticas sobre a necessidade de se repensar o conceito de privacidade em ambientes digitais, considerando a crescente presença de dispositivos conectados e a coleta massiva de informações pessoais.

Como método, utilizou-se o método de procedimento monográfico, baseado em pesquisas por documentação indireta em pesquisas precedentes e como método de abordagem o dedutivo, partindo da perspectiva geral do desenvolvimento das tecnologias, passando pela liberdade e a situação de sua relação com a proteção de dados e os instrumentos normativos vigentes.

Inicialmente- far-se-á um percurso teórico sobre o desenvolvimento das novas tecnologias e os conceitos da Sociedade de Risco e de metamorfose digital, propostos por Ulrich Beck, como subsídio teórico para compreensão do surgimento das novas tecnologias e dos aspectos envolvidos. Posteriormente, será tratado sobre a liberdade digital, a partir de uma releitura do modelo clássico de liberdade, para, então, tratar sobre suas relações com a proteção de dados pessoais.

2 SOCIEDADE DE RISCO E METAMORFOSE DIGITAL: PERSPECTIVAS E DESAFIOS NO AMBIENTE DIGITAL

A proposta teórica de Beck parte principalmente sobre situações envolvendo riscos biológicos, ecológicos, nucleares, etc, em relação à tecnologia. A Sociedade de Risco diz respeito à pós-modernidade, à era pós-industrial, sendo tratada como uma sociedade de incertezas, haja vista que "se está permeado por riscos desconhecidos e danos incontroláveis, em que preponderam incertezas das consequências oriundas do meio científico e tecnológico" (BAGATINI, 2018, p. 22). Nesse sentido, tem-se que

> nesta Sociedade de Riscos a ideia que guiava a Modernidade, qual seja, a de ser possível o controle dos efeitos colaterais e das decisões do homem restou em crise, razão pela qual Beck a define como uma sociedade do não-saber, porque no estágio alcançado pelo desenvolvimento tecnológico, os limites de controlabilidade dos riscos não tem se mostrado suficientes para evitar os danos que se consumam cada vez mais; ao contrário, cada aumento de saber/conhecimento/técnica tende a coincidir com o surgimento de novos riscos (LEAL, 2017, p. 41)

Nesse sentido, Machado e Guimarães (2017, p. 03) referem que a "teoria da sociedade de risco na pós-modernidade apresenta uma relação entre os processos de globalização dos riscos ecológicos e as manifestações específicas que estes podem adquirir em diferentes sociedades". Contudo, o discurso de Beck não apenas se limita aos riscos ecológicos, podendo ser utilizado para compreensão da tecnologia e seus impactos sociais, constituindo uma verdadeira chave de leitura para compreensão de nosso tempo.

Nesse sentido, afirma Germán Aller (2006, p. 23) que "la sociedad industrial del riesgo proviene de una fractura de la modernidad post sociedad industrial y la sociedad del riesgo es consecuencia de la obsoleto de la industrial". Logo, é o processo histórico posterior à modernidade e da industrialização, com suas respectivas fraturas, que marca o início das mudanças sociais marcadas pela existência de riscos, pois,

> [...] assim como no século XIX a modernização dissolveu a esclerosada sociedade agrária estamental, e, ao depurá-la, extraiu a imagem estrutural da sociedade industrial, hoje a modernização dissolve os contornos da sociedade industrial e, na continuidade da modernidade, surge uma nova configuração social (BECK, 2011, p. 12-13)

Quando se fala em riscos, observa-se que esses, além de não serem igualmente distribuídos, são também desconhecidos a longo prazo (BECK, 2011) e que, com a modernidade, passaram a assumir um caráter global, ocasionando a existência de situações de ameaça global, diversamente do sentido de que os riscos possuíam em períodos históricos anteriores (BECK, 2011, p. 25). Importante fazer a ressalva de que riscos não são danos, mas a probabilidade deles ocorrerem. Na leitura da tecnologia, inúmeros são os riscos invisíveis. Nesse sentido:

> A teoria da sociedade mundial do risco parece nascer com a percepção social dos riscos tecnológicos globais e de seu processo de surgimento até então despercebido. É uma teoria política sobre as mudanças estruturais da sociedade industrial e, ao mesmo tempo, sobre o conhecimento da modernidade, que faz com que a sociedade se torne crítica de seu próprio desenvolvimento. (MACHADO, 2005, p. 31)

No mesmo sentido, Machado e Guimarães (2017, p. 06) ressaltam que a teoria da Sociedade de Risco apresenta um conceito sobre a "nova modernidade (Pós-Modernidade), que opera mudanças drásticas na política, na economia e no comportamento, na medida em que a produção social de riquezas se faz acompanhar, cada vez mais, de uma produção social de riscos". Por sua vez, Aller (2006, p. 26) refere que a Sociedade de Risco diz respeito a "una característica del desarrollo de la sociedad moderna que exhibe la dinámica de la creación de riesgos de diversos órdenes: políticos, colectivos, individuales, ecológicos y seguridade entre otros, que escapan al control social contemporâneo".

Leal (2017, p. 93) aduz que "nessa Sociedade, os riscos sociais, políticos e econômicos tendem a escapar do controle institucional ordinário do Estado. As próprias instituições privadas e de mercado começam a criar riscos que não podem tampouco controlar", ou seja, o Estado tem dificuldade na controlabilidade dos riscos, de modo que sua afirmação, sendo necessária, se faz mais difícil.

Logo, a partir do descontrole dos riscos é que se insere a noção de efeito bumerangue dos riscos produzidos, mesmo diante de um padrão de sua distribuição. Beck (2011, p. 44) afirma que "nem os ricos e poderosos estão seguros diante deles [...] Os atores da modernização acabam, inevitável e bastante concretamente, entrando na ciranda dos perigos que eles próprios desencadeiam e com os quais lucram".

Aller (2006, p. 23), sobre o efeito bumerangue, que ele "destroza el esquema de clases, porque los riesgos se expanden y se acumulan [...], apareciendo un destino adscriptivo de peligro del que no hay aparente manera de escapar". Ou seja, mesmo os atores sociais responsáveis pela criação/produção dos riscos estão suscetíveis de serem atingidos pelos riscos que eles mesmos criaram, posto que na Sociedade de Risco, as classes, apesar de serem responsáveis pela sua produção, são aniquiladas, demonstrando um efeito igualador no tocante às consequências.

Com a mudança da modernidade e dos próprios riscos originados a partir da modernidade reflexiva, o modo como tem sido buscado o controle dos riscos não tem se mostrado devidamente eficiente para evitar e prevenir os danos decorrentes de tais riscos

(LEAL, 2017, p. 41), fazendo-se necessária uma reorganização/recontextualização das instituições e do Estado para se administrar tais riscos. Aqui, grande parte dessa reorganização perpassa sobre o papel dos direitos fundamentais e sua eficácia vertical e horizontal.

Portanto, a modernidade não apenas elevou a categoria dos riscos, mas demonstrou a necessidade de se reconceitualizar determinados conceitos a partir dos novos riscos gerados. Nesse sentido, Beck (2011, p. 57) afirma que "a sociedade de risco dispõe, nessa medida, de novas fontes de conflito e de consenso", referindo, a partir de um paralelo com a sociedade erigida em classes, como a sociedade industrial, que "enquanto as sociedades de classes são organizáveis em Estados Nacionais, as sociedades de risco fazem emergir 'comunhões de ameaça' objetivas, que em última instância somente podem ser abarcadas no marco da sociedade global" (BECK, 2011, p, 57), novamente sendo demonstrado o caráter global dos riscos existentes. Nesse ponto, nota-se que

> [...] a *globalização* se evidencia em face dos processos pelos quais os Estados Nacionais soberanos se misturam e se sobrepõem mediante atores transnacionais e suas respectivas probabilidades de poder. Assim, o conceito de globalização vem descrito como um processo que cria vínculos e espaços sociais transnacionais, revaloriza culturas locais e traz em primeiro plano outras culturas [grifo do autor] (LEAL, 2017, p. 46)

Nesse sentido, Ulrich Beck propõe a noção de metamorfose digital, fenômeno que, para o autor, difere de uma revolução, considerando que diz respeito a efeitos colaterais que não foram intencionados pelos indivíduos, fazendo surgir a ligação entre os ambientes online e off-line (BECK, 2018, p. 190). Essa perspectiva em muito se assemelha ao que refere Zuboff (2020, p. 9), para quem as novas tecnologias com capitalismo de vigilância é "uma nova ordem econômica que reivindica a experiência humana como matéria-prima gratuita para práticas comerciais dissimuladas de extração, previsão e vendar".

Na esteira da lição de Beck, todos esses fatores fazem com que os riscos globais se emancipem com os efeitos colaterais e, mais, fazem a expectativa de um humanismo

digital, cuja base é a proteção dos dados pessoais e os direitos de liberdade diante do fato de que as pessoas são consideradas dados em um oceano de dados (BECK, 2018, p. 190-192). Portanto, a metamorfose difere da revolução, pois essas modificações sociais não foram planejadas ou intencionadas, mas foram, simplesmente, ocorrendo.

Segundo Beck (2018, p. 187), essa perspectiva passa por encarar um dever de proteção de dados como um "supremo direito humano internacional" e encarar os riscos globais a partir de uma realidade cosmopolita (BECK, 2018, p. 189), que se visualiza como ampliar a nível global os marcos regulatórios protetivos sobre dados pessoais. Quando se fala da realidade digital, tem-se que se trata de um risco imaterial e de difícil percepção, de forma que o Estado, diante dessa realidade, não tem se mostrado suficiente no seu controle (BECK, 2018, p. 186).

O caráter global, a forma de controle dos riscos, a existência das ameaças, o próprio efeito bumerangue, são, portanto, marcas da Sociedade de Risco, não se podendo evitar a existência deles, aliados à noção de metamorfose digital.

3 LIBERDADE DIGITAL: PERSPECTIVAS E DEBATES NECESSÁRIOS

A liberdade talvez seja o mais abrangente dos direitos fundamentais e também aquele historicamente mais reivindicado, tendo em vista que abarca as mais diversas searas da expressão humana. Um dos primeiros documentos de direitos humanos de nossa era, qual seja a *Magna Carta*, de 1215 (Carta Magna das Liberdades), trouxe a liberdade como grande fator para a limitação do poder político diante do abusivo poder monárquico (COMPARATO, 2019, p. 83). Percebe-se que as primeiras reivindicações sobre a liberdade justamente diziam respeito a um tipo de afastamento da intervenção do poder estatal, ou seja, em um sentido negativo, para que o Estado deixasse de intervir na liberdade pessoal (o que também muito tem ligação com um conceito clássico de privacidade, que será abordado posteriormente). Parte da doutrina entende que essa ideia geral de liberdade se vincula ao grupo dos chamados direitos de defesa:

> A clássica concepção de matriz liberal-burguesa dos direitos fundamentais informa que tais direitos constituem, em primeiro plano, direitos de defesa do indivíduo contra ingerências do Estado em sua liberdade pessoal e propriedade. Esta concepção de direitos fundamentais – apesar de ser pacífico na doutrina o reconhecimento de diversas outras – ainda continua ocupando um lugar de destaque na aplicação dos direitos fundamentais. Esta concepção, sobretudo, objetiva a limitação do poder estatal a fim de assegurar ao indivíduo uma esfera de liberdade. Para tanto, outorga ao indivíduo um direito subjetivo que permite evitar interferências indevidas no âmbito de proteção do direito fundamental ou mesmo a eliminação de agressões que esteja sofrendo em sua esfera de autonomia pessoal (MENDES, 1999, p. 2)

Ou seja, seria a liberdade um direito que possibilitaria em larga escala a fruição dos demais direitos fundamentais. A história demonstra que essa concepção negativa, na ideia de não intervenção, pouco a pouco se mostrou insuficiente frente aos anseios sociais. As lutas pelos direitos consagraram, então, a ideia de que não bastava apenas o Estado se eximir de interferências, mas deferia agir positivamente para assegurar o exercício dos direitos, nomeadamente o direito de liberdade. Nesse sentido:

> Vinculados à concepção de que ao Estado incumbe, além da não-intervenção na esfera da liberdade pessoal dos indivíduos, garantida pelos direitos de defesa, a tarefa de colocar à disposição os meios materiais e implementar as condições fáticas que possibilitem o efetivo exercício das liberdades fundamentais, os direitos fundamentais a prestações objetivam, em última análise, a garantia não apenas da liberdade-autonomia (liberdade perante o Estado), mas também da liberdade por intermédio do Estado, partindo da premissa de que o indivíduo, no que concerne à conquista e manutenção de sua liberdade, depende em muito de uma postura ativa dos poderes públicos (MENDES, 1999, p. 3).

Dessa maneira, o exercício do direito de liberdade, dentro da evolução dos direitos fundamentais, foi um dos protagonistas na busca pela limitação do poder e consagração dos direitos individuais. Essa visão do direito de liberdade é fruto da tradicional visão dos direitos fundamentais, ligados a padrões de observação e pensamento, típica dos paradigmas liberais (ALBERS, 2016, p. 21). Essa concepção "como proteção contra violações de direitos ou ingerências neles parece ser uma proteção abrangente e ótima da

liberdade" (ALBERS, 2016, p. 13), mas que sofre transformações diante da complexização social e jurídica decorrente de uma proteção de dados pessoais.

Da leitura da Constituição da República de 1988, percebem-se as inúmeras referências ao direito de liberdade, inclusive como objetivo fundamental da República na constituição de uma sociedade livre (BRASIL, 1988). É no artigo 5º que se encontram as maiores referências a esse direito, quando se trata da ideia de um amplo direito de liberdade limitado apenas por lei, conforme o inciso I, ou como liberdade de manifestação do pensamento, na esteira do inciso IV, e de liberdade de locomoção, garantida, entre outros, pelo inciso XV (BRASIL, 1988).

Nesse sentido, na seara dos tratados internacionais e de direitos humanos a liberdade também assume importância notável nesses documentos. Uma das principais referências é a Declaração Universal dos Direitos Humanos, que resguarda a liberdade nos artigos, dentre outros, 1º, 2º e 3º (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 1948). Além disso, observa-se que a Convenção americana de Direitos Humanos também traz alguns postulados sobre o direito de liberdade, notadamente em seu artigo 7º (ORGANIZAÇÃO DOS ESTADOS AMERICANOS, 1969). Isso demonstra a importância assumida pelo direito de liberdade, seja em âmbito nacional como internacional, e a devida proteção que esse direito deve ter.

Para José Afonso da Silva (2017, p. 235), a liberdade seria a "possiblidade de coordenação consciente dos meios necessários à realização da felicidade pessoal" e, nesse sentido, para o autor, se apresentaria em cinco grandes grupos na atual ordem constitucional: liberdade da pessoa física, liberdade de pensamento, liberdade de expressão coletiva, liberdade de ação profissional e liberdade de conteúdo econômico e social (SILVA, 2017, p. 237).

As liberdades, nesse sentido, possuem espécies próprias como, por exemplo, a liberdade de expressão, de locomoção, consciência, etc, que possuirão âmbitos de proteção com conteúdos também próprios a partir da peculiaridade do direito em espécie, cujos limites também corresponderão ao direito em questão. Além disso, importante considerar que as disposições constitucionais acerca das liberdades possuem eficácia

plena e são diretamente aplicáveis (SILVA, 2017, p. 270), especialmente considerando que esse direito fundamental tem ainda mais relevo em uma sociedade democrática, que é seu campo de exercício (SILVA, 2017, p. 236).

Considerando a proposta do presente estudo, as espécies de direitos de liberdade serão aqui estudadas de modo exemplificativo, sempre tendo em mente o direito geral de liberdade, dado que, com a Internet, sofreram mudanças em suas formas de manifestação e também de violação. Com isso, é possível entender de que maneira essa nova formação social acarreta mudanças específicas no agir humano e, consequentemente, no exercício das liberdades.

O estudo da liberdade pessoal e de circulação no ambiente erigido a partir da difusão Internet permitirá uma análise profunda desses direitos dentro do contexto mencionado. Trata-se de um questionamento que Rodotà já fazia sobre como a liberdade de circulação se impostaria no ambiente digital, aliado a outras liberdades, como a de expressão e de associação, que serão indiretamente abordados (RODOTÀ, 2008, p. 200).

Veja-se que tal espécie toma duas frentes diferentes com o ambiente digital: seja por meio da vigilância constante, permeando a nossa liberdade, seja pela liberdade de circulação no interior da própria Internet. Além disso, será analisado o nominado direito ao livre desenvolvimento da personalidade, que apesar de estar relacionado ao rol dos direitos de personalidade, é "um direito de liberdade, no sentido de um direito de qualquer pessoa a não ser impedida de desenvolver sua própria personalidade e de se determinar de acordo com suas opções" (SARLET; MARINONI; MITIDIERO, 2017, p. 439), noção que também decorre da ampliação do direito de liberdade na Constituição.

Certamente, a questão sobre uma forma de liberdade de circulação na Internet traz inúmeros debates e reflexões. No entanto, se tomado em conta que a forma clássica desse direito não se visualiza suficiente para uma adequada proteção diante da formação de perfis informáticos, direcionamentos de conteúdo a partir da captação de superávit comportamental para segmentação comportamental da pessoa, por exemplo, é visível que o questionamento de Rodotà (2008, p. 200), a partir da Constituição Italiana, de "qual é o alcance da liberdade de circulação (art. 16) na presença da vigilância por vídeo e difusão

das técnicas de localização?" e de se "as garantias da liberdade pessoal (art. 13) devem ser também estendidas ao corpo 'eletrônico, seguindo a trajetória da releitura do *habeas corpus* como *habeas data*?" (grifo do autor), assume importância para debate na seara dos direitos fundamentais.

Os ativistas virtuais Julian Assange, Jacob Appelbaum, Andy Müller e Jérémie Zimmermann, em obra coletiva, trataram do tema liberdade de circulação com preocupação diante da massiva vigilância estatal. Para Assange, três liberdades são fundamentais, quais sejam a de comunicação, circulação e de interação econômica. Acrescenta-se a essa ideia, nas palavras do autor, que

> Se olharmos para a transição da nossa sociedade global para a internet, quando fizemos essa transição a liberdade de circulação pessoal permaneceu basicamente inalterada. A liberdade de comunicação foi enormemente expandida em alguns aspectos, no sentido de que agora podemos nos comunicar com um número muito maior de pessoas; por outro lado, ela também foi enormemente reduzida, porque não temos mais privacidade e as nossas comunicações podem ser interceptadas, armazenadas e, como resultado, usadas contra nós. Então a interação elementar que temos fisicamente com as pessoas acabou se degradando (ASSANGE; *et al*, 2013, p. 89).

A liberdade de expressão, para eles, assumiu novos contornos diante das devassas à privacidade. Todavia, não somente nesse contexto, posto que a ampliação da possibilidade de expressão permitiu outras formas de violação a outros direitos. Conforme trazem Mendes e Fernandes (2020, p. 7), o aumento dos espaços de fala permitidos pela Internet "torna a liberdade um campo fértil para diversas formas de abusos, o que pode ser percebido na disseminação de discursos odiosos, *cyberbullying*, pornografia infantil e mesmo na difusão em massa de notícias falsas".

Contudo, a linha adotada pelos ativistas virtuais trata nomeadamente da vigilância estatal e de riscos a ela associados. Nesse sentido, é plausível que a interceptação da comunicação privada realizada através da Internet ilegalmente afeta de alguma maneira o direito à liberdade de comunicação, tendo em vista que a inviolabilidade das comunicações privadas constituiu uma garantia fundamental do cidadão (STRECK, 1997,

p.17). Essa garantia, no ambiente digital, não se estende tão somente contra as violações estatais, mas também a causada por entes privados, nomeadamente agentes econômicos da Internet. Jacob Appelbaum acrescenta que, em verdade, os espaços de expressão no mundo real também se viram limitados pelas restrições à liberdade de circulação, pois, nas palavras do autor,

> Se formos seguir essa noção reducionista da liberdade, das três liberdades que Julian mencionou, isso é claramente vinculado à liberdade de circulação – hoje em dia não dá nem para comprar uma passagem de avião sem usar uma moeda rastreável, caso contrário a transação é imediatamente sinalizada. Se você entrar em um aeroporto e tentar comprar uma passagem para o mesmo dia com dinheiro vivo, você é imediatamente visado e será forçado a passar por revistas de segurança extra, não poderá voar sem identificação e, se tiver a infelicidade de comprar sua passagem com um cartão de crédito, eles registrarão tudo – desde o seu endereço IP até o seu navegador. (ASSANGE; *et al*, 2013, p. 99)

Se visualizada a teoria dos direitos fundamentais, sob a análise do direito de liberdade em espécie, verifica-se que a noção sobre a liberdade frente às tecnologias permite de uma releitura. Trata-se de direito que possui duas dimensões de seu âmbito de proteção. Em uma concepção subjetiva, é o direito de defesa de não se ver restringido na livre circulação e locomoção, sem que haja qualquer tipo de embaraço (SARLET; MARINONI; MITIDIERO, 2017, p. 527-528). De outro lado, a acepção objetiva é facilmente extraída a partir dos elementos de base antes vistos, posto que se trata de um dever do Estado de assegurar o exercício desse direito de liberdade, garantindo os meios materiais para esse exercício.

Assim, sendo direito fundamental de suma importância, os novos riscos associados à Internet e novas tecnologias e a liberdade exigem uma proteção maior e suficiente, tendo em vista que a violação da liberdade é diferente dos outros direitos fundamentais e dos riscos globais, uma vez que o risco a ela possui uma ameaça imaterial (BECK, 2018, p. 186). Essa proteção, na seara constitucional, perpassa por uma ampliação da materialização do dever de proteção estatal, por exemplo, através da via legislativa e atuação de autoridades voltadas à proteção desses direitos.

No Brasil, há uma proteção jurídica mínima para a liberdade no ambiente digital, como se verá adiante, principalmente com o Marco Civil da Internet e a Lei Geral de Proteção de Dados Pessoais, perpassando essa proteção por uma proteção de dados pessoais. Todavia, ela não se mostra atualmente suficiente. A uma, pois o Brasil caminha a passos lentos para a compreensão da proteção aos direitos fundamentais no ambiente digital, bastando-se ver que a proteção iniciou há pouco mais de uma década e a dificuldade na efetiva atuação da Autoridade Nacional de Proteção de Dados Pessoais, recentemente instituída. A duas, pois a Internet, a nível mundial, é regulada de distintas maneiras, que por vezes podem dificultar uma correta proteção à liberdade de circulação, por exemplo. Vale lembrar que esse direito, assim como os direitos fundamentais em geral, não se mostra absoluto, dado que podem sofrer restrições permitidas pela legislação, como, por exemplo, pela segurança pública. No entanto, assim como a legislação para o ambiente digital em geral, esse desenvolvimento ainda se mostra tímido.

Conceito diferente é a ideia de liberdade informática, que é tratada como "um direito específico de conhecimento e controle de dados pessoais" (DONEDA, 2019, p. 170). Frosini (2003, p. 30) ressalta que se trata de um novo instituto oriundo, sobretudo, da sociedade tecnológica, constituindo um avanço para a fronteira da liberdade humana através da sociedade. No entanto, também entende que manter as formas tradicionais de liberdade seria forçado, representando a liberdade informática como uma nova liberdade constitucional da sociedade tecnológica (FROSINI, 2003, p. 31-32).

Decorre daí a afirmativa de Rodotà (2008, p. 200) para quem, a partir da situação desse novo ambiente e a Constituição Italiana, se impõe uma "reconstrução dos direitos e liberdades referentes ao ambiente tecnológico no qual são exercidos". Alguns autores chegam a definir a liberdade na Internet como um desafio nesse contexto, argumentando que:

> As redes da Internet propiciam comunicação livre e global que se torna essencial para tudo. Mas a infraestrutura das redes pode ter donos, o acesso a ela pode ser controlado e seu uso pode ser influenciado, se não monopolizado, por interesses comerciais, ideológicos e políticos. À medida que a Internet se torna a infraestrutura onipresente de nossas vidas, a questão de quem possui e

> controla o acesso a ela dá lugar a uma batalha essencial pela liberdade (CASTELLS, 2003, p. 226)

Tanto se tornou presente nas vidas que Beck (2018, p. 190) enuncia o fenômeno da metamorfose digital, assentando o "entrelaçamento essencial do on-line e do off-line", em alusão à influência que a Internet e a informática exercem nas vidas. No entanto, diga-se ainda que, para Castells (2003, p. 225) o modo como a Internet vem sendo conduzida é passível de gerar um verdadeiro efeito bumerangue (CASTELLS, 2003, p. 225). A afirmativa é reforçada, como visto acima, pela concepção de capitalismo de vigilância, trazida por Zuboff (2020).

4 A LIBERDADE DIGITAL E SUA RELAÇÃO COM A PROTEÇÃO DE DADOS PESSOAIS NO AMBIENTE DIGITAL

O direito sobre a proteção dos dados pessoais é tema discutido há pouco tempo no Brasil, de forma que as normas que disciplinam o tratamento de dados pessoais, principalmente na Internet, são recentes. Percebe-se que o direito fundamental correspondente somente foi consagrado de modo expresso na Constituição no ano de 2022, inserindo-o no rol do artigo 5º a disciplina da proteção de dados pessoais em caráter fundamental (BRASIL, 1988).

A concepção de que o direito à proteção de dados pessoais é fundamental e que não se engloba no conceito de direito à privacidade é construção teórica recente que se iniciou a partir do desenvolvimento das tecnologias da informação, de modo que a mera concepção da privacidade, seja como direito a estar só ou como direito ao controle dos dados e informações, não se mostrava suficiente. Esse foi o entendimento do Supremo Tribunal Federal por ocasião do julgamento da ADI 6387 (BRASIL, 2020), quando a Corte, pela primeira vez, se pronunciou sobre o caráter fundamental desse direito, em julgamento que tratava sobre a tese da inconstitucionalidade da Medida Provisória 954/2020, eis que violava o sigilo e a proteção dos dados.

A referida medida dizia respeito à obrigatoriedade de compartilhamento dos dados telefônicos das operadoras ao IBGE durante a pandemia de COVID-19 (BRASIL, 2020, p. 02). Em seu voto, afirmou o Ministro Gilmar Mendes que o direito fundamental à proteção de dados pessoais "não mais se adstringe à demarcação de um espaço privado, mas, antes, afirma-se no direito à governança, transparência e sindicabilidade do tratamento de dados compreendidos em acepção abrangente" (BRASIL, 2020, p. 20). No mesmo sentido, declarou:

> A afirmação da autonomia do direito fundamental à proteção de dados pessoais – há de se dizer – não se faz tributária de mero encantamento teórico, mas antes da necessidade inafastável de afirmação de direitos fundamentais nas sociedades democráticas contemporâneas.
> Considerando que os espaços digitais são controlados por agentes econômicos dotados de alta capacidade de coleta, armazenamento e processamento de dados pessoais, a intensificação do fluxo comunicacional na internet aumenta as possibilidades de violação de direitos de personalidade e de privacidade (BRASIL, 2020, p. 21).

De outro lado, diversos outros países já reconheciam o caráter jusfundamental da proteção de dados pessoais em suas Constituições. Trata-se de um movimento internacional que, reconhecendo a importância jurídica dos dados pessoais e os riscos possíveis à liberdade humana, busca proteger os cidadãos no ambiente virtual.

Exemplo de uma das experiências mais sólidas e reconhecidas sobre a proteção de dados pessoais em todos os seus contornos é a da Itália. Muito bem desenvolvido pelo jurista italiano Stefano Rodotà, o sistema de proteção criado pela Itália em muito inspirou o brasileiro (LIMA, 2020, p. 169). Semelhantemente ao Brasil, a legislação italiana disciplina o tratamento dos dados pessoais a partir da noção de dignidade humana, que é muito cara ao direito brasileiro (LIMA, 2020, p. 175). Nesse sentido, o sistema italiano em muito observa os ditames do continente europeu e o modo como a Europa trata sobre a proteção de dados, sobretudo a partir da criação do GDPR.

Com isso, o pano de fundo de todo o ordenamento é considerar o direito à proteção de dados pessoais como um direito fundamental, que está previsto na Carta de Direitos Fundamentais da União Europeia, em seu artigo 8º. Inclusive, Rodotà defende que tal

direito deve ser visto em um contexto ainda mais amplo que o que prevê a Carta de Direitos Fundamentais, sobretudo em razão dos direitos que surgem a partir do desenvolvimento das tecnologias (RODOTÀ, 2008, p. 17).

Sem pretender traçar um estudo de direito comparado ou adentrar nos regramentos próprios no âmbito internacional, denota-se que as experiências estrangeiras em muito acrescentam para a possibilidade de se tracejar uma proteção em unidade a nível global, principalmente diante do caráter global da Internet. As relações entre a LGPD e o GDPR evidenciam essa possibilidade e necessidade. Todavia, importante destacar a lição de Silveira e Froufe sobre a realidade da União Europeia e de seu sistema de proteção quando afirmam que

> RGPD concretiza a solução adotada pela CDFUE quando autonomizou o direito à proteção de dados pessoais (art. 8.º) relativamente ao direito à proteção da vida privada (art. 7.º). Para o direito da União Europeia nem todos os dados pessoais são suscetíveis, pela sua natureza, de causar prejuízo à privacidade da pessoa em causa – mas devem ser igualmente protegidos. (SILVEIRA; FROUFE, 2018, p. 20).

Para tais autores, a relação entre a questão jurídica e "a proteção de dados pessoais converteu-se na questão jusfundamental identitária dos nossos tempos para que o projeto do humanismo não se torne irrelevante" (SILVEIRA; FROUFE, 2018, p. 7). Trata-se daquilo que Beck (2018, p. 190) afirmou como expectativa e efeito colateral do risco global, qual seja a necessidade de um "humanismo digital", pautado nos ideais da liberdade e da proteção de dados pessoais.

Aliás, é essa a concepção que faz com que se busque descolar a visão de dados pessoais como algo estático em razão da existência das complexidades que lhe são inatas. Inclusive, o direito fundamental à proteção de dados é direito indisponível, cuja perspectiva faz descolar da ideia de dados pessoais como propriedade, ainda mais diante dos meios virtuais e da forma econômica que os dados vêm assumindo.

No âmbito do ordenamento constitucional pátrio, a tramitação a PEC 17/2019 junto ao Poder Legislativo Brasileiro, constituiu importante virada de chave na seara dos direitos fundamentais diante das novas tecnologias. O trâmite da proposta fez com que a

Constituição da República incorporasse ao seu texto e reconhecesse expressamente um direito que antes era visto de modo implícito. Assim, denota-se que "a experiência legislativa segue justamente nessa direção, confirmando como é impossível prescindir de uma estratégia institucional articulada e integrada" (RODOTÀ, 2008, p. 81), devendo constituir efetiva atuação estatal na gestão e criação dos mecanismos necessários de regulação das práticas do ambiente da informação, que transcendem as fronteiras e a soberania de qualquer Estado, sendo a proteção desse direito em âmbito constitucional efetiva possibilidade de uma proteção articulada e integrada, como pretendia Rodotà.

O autor italiano ainda afirma que "a proteção de dados estabelece regras sobre os mecanismos de processamento de dados e estabelece a legitimidade para a tomada de medidas – *i.e.* é um tipo de proteção dinâmico, que segue o dado em todos os seus movimentos" (RODOTÀ, 2008, p. 17). Nesse sentido, verifica-se que:

> A proteção dos dados pessoais alcançou uma dimensão sem precedentes no âmbito da sociedade tecnológica, notadamente a partir da introdução do uso da tecnologia da informática. [...] A facilidade de acesso aos dados pessoais, somada à velocidade do acesso, da transmissão e do cruzamento de tais dados, potencializa as possibilidades de afetação de direitos fundamentais das pessoas, mediante o conhecimento e o controle de informações sobre a sua vida pessoal, privada e social." (SARLET; MARINONI; MITIDIERO, 2017, p. 472).

Diante disso, é possível afirmar que o novo "direito fundamental exorbita aquele protegido pelo direito à privacidade, pois não se limita apenas aos dados íntimos ou privados, ao revés, refere-se a qualquer dado que identifique ou possa identificar um indivíduo" (MENDES; FONSECA, 2020, p. 473), lembrando-se sempre que o aspecto do dado não se relaciona com o aspecto de um direito de propriedade, mas da própria individualidade da pessoa, ou seja, de sua personalidade.

Além disso, há que se destacar a necessária proteção do desenvolvimento da pessoa a partir dos meios tecnológicos e de possíveis conflitos que surgem a partir de então, demonstrando a necessidade de uma adequada proteção. Logo,

> Nos dias atuais, os aspectos da tutela da privacidade e intimidade encontram-se muito integrados com a proteção de dados pessoais, pelo fato de que tais dados representam pressupostos irrenunciáveis ao desenvolvimento da pessoa humana e, ao mesmo tempo, estão conectados com demandas de mercado, pois alimentam infindáveis segmentos de atividades industriais e comerciais que pagam valores imensos por informações de seus consumidores, formatando-se, neste âmbito, zonas de potenciais conflitos entre interesses distintos (LEAL, 2020, p. 366).

Afirma-se, portanto, que o direito fundamental à proteção de dados pessoais possui um âmbito de proteção próprio que também se evidencia na dimensão objetiva, gerando o dever estatal de tutela. Sarlet pontua que "ao Estado incumbe um dever de proteção a ser concretizado mediante prestações normativas e fáticas, notadamente, por meio da regulação infraconstitucional dos diversos aspectos relacionados às posições jusfundamentais" (SARLET; MARINONI; MITIDIERO, 2017, p. 474).

No ambiente virtual, o Estado deve reassumir o seu protagonismo na garantia dos direitos fundamentais, pois o "risco à liberdade digital ameaça 'somente' algumas das principais conquistas da civilização moderna: liberdade e autonomia pessoais, privacidade e as instituições básicas da democracia e do direito, todas baseadas no Estado-nação" (BECK, 2018, p. 187). Beck (2018, p. 188) ainda refere que há a formação de verdadeiro poder central digital autônomo, travestido de uma fachada democrática.

Rodotà (2008, p. 201) afirma que "não se pode postular a indiferença do quadro tradicional dos direitos a este novo ambiente, mantendo inalterados os critérios hermenêuticos pré-tecnológicos". De todo modo, as imbricações estão presentes, tendo-se essa perspectiva ou não. Veja-se, por outro lado, que a proteção de dados pode ser geradora de uma liberdade, tendo em vista que:

> os direitos fundamentais como base da proteção de dados não resultam na obrigação de entender as leis sobre o pano de fundo do papel tradicional delas. Além de permitir o desenvolvimento de novos bens juridicamente tutelados, os direitos fundamentais permitem uma compreensão multidimensional das reservas e das regulamentações. As normas jurídicas não só limitam liberdades. Elas também podem, antes de tudo, criar liberdades, torná-las concretas e influenciar suas condições e pré-requisitos sociais. O direito referente à proteção de dados deve estar fundamentado nas diversas funções e diversas formas do direito (ALBERS, 2016, p. 39).

Por trás de toda a perspectiva desse direito, reside uma grande complexidade que permeia diversos outros direitos fundamentais já consagrados, de forma que a proteção aos dados pessoais não se mostra, diante da Era da Informação e da Sociedade de Riscos, um direito desatento aos demais direitos fundamentais.

Albers (2016, p. 29-30), quando trata da complexidade da proteção de dados pessoais, aduz que a disciplina da proteção de dados não busca proteger tão somente os dados, mas os indivíduos aos quais aqueles dados se referem, não sendo uma concepção isolada apenas dos dados, de caráter individualista.

Trata-se, então, de uma necessidade de "compreensão multidimensional de direitos fundamentais; e, em decorrência disso, a proteção de dados inclui um conjunto de direitos que precisam ser descritos de uma maneira nova" (ALBERS, 2016, p. 33), de forma que os indivíduos possam ter conhecimento dos dados, obter a informação, participar e influenciar nas questões relativas aos dados pessoais (ALBERS, 2016, p. 34).

O direito à proteção de dados pessoais não se trata de um direito instrumental visto tão somente como protetor de outros direitos, mas de "um conjunto complexo de interesses dignos de tutela" (ALBERS, 2016 p. 38), cuja compreensão deve ser "multidimensional de direitos fundamentais e exige descrições inteiramente novas dos interesses protegidos" (ALBERS, 2016, p. 38).

Essa perspectiva de se encarar o direito fundamental em questão é uma virada de chave em uma economia informacional, onde o dado pessoal, em verdade, é visto como uma mercadoria. Daí a afirmativa de Rodotà de que "o direito à proteção de dados tem a ver com a proteção da personalidade, não da propriedade" (RODOTÀ, 2008, p. 19).

Diante disso, denota-se que, na Sociedade de Risco, visualizada a partir da perspectiva da metamorfose digital, uma ampla proteção aos dados pessoais é não somente um resguardo, mas uma verdadeira necessidade. Nesse sentido, visualizar esse direito em ampla perspectiva é passo necessário para alçar o caráter fundamental e de uma verdadeira cidadania eletrônica (RODOTÀ, 2008, p. 145). No mesmo contexto:

> A proteção de dados baseia-se em uma compreensão multidimensional de direitos fundamentais e exige descrições inteiramente novas dos interesses protegidos: em vez de bens juridicamente tutelados concebidos de modo individualista, a questão tem a ver com posições jurídicas individuais na socialidade ou, em outras palavras, as posições sociais do indivíduo a serem protegidas por direitos fundamentais. O conjunto de interesses e posições protegidos ainda precisa ser elaborado com maior grau de detalhamento e também terá de ser sempre adaptado dinamicamente a novos perigos (ALBERS, 2018, p. 38).

Dessa maneira, a perspectiva cosmopolita do risco digital é importante passo na questão dos dados pessoais (BECK, 2018, p. 194), ainda mais quando visualizada também sob o aspecto do devido processo informacional na sua relação do Estado e dos particulares. A quantidade de dados produzidos em caráter global por diversos indivíduos ao redor do planeta evidencia essa necessidade de se encarar a proteção jurídica mediante instrumentos que possuam efetividade e, sobretudo, visualizar padrões mínimos mundiais de proteção e regulamentação. Nesse sentido, a diretriz de "coletar tudo" (BECK, 2018, p. 193) impõe uma ampla e fortalecida proteção, haja vista que destitui princípios básicos da liberdade (BECK, 2018, p. 193). Nesse contexto:

> A legislação precisa regulamentar o processamento de dados de modo apropriado e garantir que o tratamento de informações e dados pessoais não ocorra de maneira irrestrita, ilimitada e intransparente, e tem de assegurar que os indivíduos afetados tenham a possibilidade de obter conhecimento suficiente sobre o processamento de dados e informações pessoais e influência suficiente sobre ele. Neste nível, a presença do Estado é imprescindível (ALBERS, 2016, p. 38)

Não é à toa que Marion Albers (2016, p. 44) enuncia que esse direito "à proteção de dados é uma área nova e altamente complexa do direito que ainda precisa de um considerável aprofundamento no tocante ao seu assunto, aos interesses protegidos e aos conceitos apropriados para a regulamentação".

Diante disso, o fenômeno trazido por Beck, da Sociedade de Risco diante de uma metamorfose digital, faz sobressair a importância da proteção de dados pessoais, especialmente diante dos riscos envolvidos nas relações e do impacto mundial que os dados possuem no atual estágio da tecnologia.

4 CONSIDERAÇÕES FINAIS

O presente trabalho teve por objetivo verificar em que medida a Lei Geral de Proteção de Dados brasileira, aliada ao direito fundamental à proteção de dados pessoais, podem contribuir à tutela de direitos fundamentais relacionados à pessoa na Sociedade de Risco na Era da Informação, muito especialmente em ambientes digitais, com especial enfoque no direito à liberdade.

Sob o aspecto aqui estudado, constatou-se que, sobretudo diante da metamorfose digital, a proteção de dados assumiu ponto central na evolução da Sociedade em Rede, haja vista a massiva utilização de dados para a predição comportamental, comércio eletrônico, entre outros. Essa formação social veio acompanhada de diversos riscos que, assim como os riscos ambientais, tão bem trazidos por Beck, acarretam riscos à pessoa, nomeadamente em sua liberdade.

Nesse sentido, percebeu-se que tais riscos são, de fato, incontroláveis e igualmente podem acarretar o chamado efeito bumerangue, na medida em que os seus produtores podem ser atingidos pelos seus efeitos. Essa lógica se amolda perfeitamente ao fenômeno aqui estudado, pois os vazamentos de dados, a vigilância constante, os riscos envolvendo dados pessoais são fatores presentes nessa "nova" Sociedade de Risco digital. Surge, então, a necessidade de se falar na reestruturação do Estado e das normas para se proteger o indivíduo nesse ambiente, especialmente diante dos riscos existentes.

Denota-se que é necessária a releitura da liberdade à luz das novas tecnologias, principalmente na formação do corpo eletrônico e de sua tutela. Nesse sentido, evidencia-se a tutela da liberdade em seus mais variados aspectos, seja a liberdade na vida real, mitigada frente ao uso de georreferenciamento, GPS, controles de informações, seja no ambiente digital, considerando a formação do corpo eletrônico e na mitigação de informações à disposição do usuário na rede, especialmente através da segmentação comportamental.

Nesse cenário, constatou-se que buscar o socorro do direito à privacidade em grande medida não se mostra, por si só, suficiente na proteção do indivíduo no espectro

societal aqui analisado. A pesquisa evidenciou que, apesar de ser um direito sempre atento às realidades e com grande elasticidade, os conceitos e posições jurídicas atuais lançam a tutela necessária para o novel direito à proteção de dados pessoais. Em verdade, há uma espécie de esgotamento da tutela da privacidade nesse ambiente, de modo que seu âmbito de proteção se mostra reduzido e impossibilitado de tutelar a pessoa no ambiente digital, sobretudo nos panoramas de risco que a envolvem.

Nesse sentido, observou-se que a referida lei se assenta em concretos princípios norteadores do tratamento de dados, caracterizando-se como uma verdadeira lei norteadora e central no que tange às relações que envolvam a temática dos dados pessoais. Ao lado do seu direito fundamental, é possível constatar que a proteção de dados pessoais se constitui com o importante direito da Sociedade de Risco no âmbito da Sociedade em Rede, sobretudo quando pautado na defesa das liberdades digitais.

O papel dos princípios, de fato, constitui um grande avanço na defesa das liberdades, pois permite a interpretação do sistema jurídico à realidade concreta, além de, como dito, nortear o tratamento e as operações envolvendo dados pessoais. Além disso, as bases legais, tidas aqui como taxativas, atuam como balizas às operações com dados pessoais, resguardando tanto a proteção ao próprio indivíduo, como assegurando o âmbito de proteção do direito de liberdade.

Nesse sentido, algumas outras possibilidades devem ser assentadas de forma propositiva como resultado das análises aqui realizadas. A primeira delas é visualizar a complexidade que se tem diante dos novos cenários decorrentes de metamorfose digital e compreender o papel fundamental que a proteção de dados tem na defesa das liberdades, do corpo eletrônico e do próprio indivíduo, inclusive como sustentáculo na proteção de diversos outros direitos. Assim, cada vez mais se tem a necessidade de entender essa complexidade sob o viés dos direitos fundamentais e do constitucionalismo digital, ou seja, sob a ótica das novas tecnologias.

Conforme analisado ao longo da pesquisa, as mudanças relacionadas ao contexto digital implicam na descrição e análise inteiramente nova de categorias e conceitos dos

direitos fundamentais, como a própria liberdade, a teoria dos direitos fundamentais, ampliando-se o leque de proteção conferido por esses direitos em nosso sistema.

Valorosa parte dessa complexidade se visualiza também na necessidade de políticas públicas relacionadas ao direito fundamental à proteção de dados. Além da própria proteção conferida pela legislação ordinária, é preciso maior esforço regulatório nesse sentido, englobando-se, inclusive, a tutela penal para os dados pessoais, de forma a se garantir uma ampla e estratégica proteção do indivíduo, especialmente no que tange ao uso de novas tecnologias para política criminal ou segurança pública.

Ademais, a criação de instrumentos específicos e mais detalhados do que a LGPD devem ser debatidos, como a regulação do mercado digital e aspectos relacionados à transferência internacional, por exemplo. Com isso, estar-se-á a concretizar o modelo de corregulação entre Estados e particulares, na medida em que o Estado fixará as balizas normativas, podendo o particular tutelar ainda mais os direitos em questão.

Outro fator que não foi devidamente trabalhado pela LGPD é a importância dos relatórios de impactos em relação aos dados pessoais, pois, para além de documentar as formas de tratamento de dados, pode constituir necessários mecanismos de governança e controlabilidade dos dados. Necessário relembrar que se está a se tratar de direitos fundamentais, cujas intervenções somente podem ser concretizadas mediante previsão legal – para fins da presente análise as bases legais, naquilo que vem se nominando como devido processo informacional.

Os relatórios de impacto se caracterizam como instrumento mediador entre o tratamento de dados pessoais e os riscos associados a essas atividades, mas que, atualmente, não dispõem de diretrizes mínimas para tanto. Isso permite que o usuário e o agente de tratamento tenham conhecimento, mesmo que mínimo, dos riscos pertinentes.

Além disso, vale destacar a importância da atuação da Autoridade Nacional na tutela das liberdades, considerando se tratar da figura estatal específica nas questões envolvendo dados pessoais, especialmente em seu papel judicante e legiferante. Afora as questões envolvendo a sua independência, o destaque necessário deve se fazer para a sua atuação sancionatória, investigativa e, principalmente, educativa, através de políticas

públicas educacionais, promovendo aquilo que se nomina como a cultura de proteção aos dados pessoais.

Os danos decorrentes dos riscos erigidos com o ambiente digital são, de fato, irrecuperáveis, considerando o modo como a sociedade se encontra globalizada. Nesse cenário de riscos, constituir elementos normativos na forma de direitos humanos, direitos fundamentais e legislações regulatórias se mostra não apenas importante, mas necessário à defesa das liberdades na atualidade, inclusive atendendo-se ao princípio da dignidade humana. Em um ambiente que cada vez mais se mostra interligado à realidade, é imperioso se visualizar os direitos fundamentais no novo ambiente, objetivando, ao fim, atender à tutela da pessoa.

Dessa forma, conclui-se que o panorama teórico aqui utilizado reforça a hipótese da importância do direito fundamental e de uma Lei Geral de Proteção de Dados Pessoais que, contudo, não esgota as possibilidades de proteção aos direitos fundamentais, diante da necessidade de discussão das proposições acima elencadas como forma de ampliar o âmbito de proteção da liberdade e da pessoa na Sociedade de Risco.

Ademais, a proteção de dados pessoais é importante baliza na discussão entre segurança e liberdade na Internet. Com isso, a regulação dos dados pessoais no Brasil constitui o ponto de equilíbrio em face das relações multifacetadas que envolvem o tema liberdade e segurança. Ora, a partir da noção pendular de Baumann, se está a conferir mais segurança no ambiente digital, se está a diminuir a proteção à liberdade e, do contrário, conferindo maior proteção à liberdade, perde-se no aspecto segurança. Percebe-se, do que foi exposto, que tratar sobre o tema proteção de dados – do qual há muito a se avançar no país – é encontrar o ponto de equilíbrio entre esses dois aspectos.

REFERÊNCIAS

ALBERS, Marion. A complexidade da proteção de dados. **Revista Direitos Fundamentais & Justiça**, a. 10, n. 35, p. 19-45, jul./dez. 2016.

ALLER, Germán. **La Sociedad del Riesgo**. In Co-responsabilidad social, Sociedad del Riesgo y Derecho penal del Enemigo. Montevideo: Carlos Álvarez-Editor, 2006.

ASSANGE, Julian. *et al*. **Cypherpunks**: liberdade e o futuro da internet. São Paulo: Boitempo
Editorial, 2013.

BAGATINI, Júlia. **O espetáculo na sociedade da informação**: política pública de Direito dos Danos por risco do desenvolvimento fundamentada no princípio constitucional da solidariedade. 2018. Tese (Doutorado em Direito) – Universidade de Santa Cruz do Sul, Santa Cruz do Sul, 2018. Disponível em: https://repositorio.unisc.br/jspui/bitstream/11624/2416/1/J%c3%balia%20Bagatini.pdf. Acesso em: 13 mar. 2023.

BECK, Ulrich. **A metamorfose do mundo***:* novos conceitos para uma nova realidade. Tradução por Maria Luiza X. de A. Borges. Rio de Janeiro: Zahar, 2018.

BECK, Ulrich. **Sociedade de risco***:* rumo a uma outra modernidade. Tradução por Sebastião Nascimento. São Paulo: 34, 2011.

BRASIL, Constituição (1988). **Constituição da República Federativa do Brasil**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/Constituicao Compilado.htm. Acesso em: 18 jan. 2023.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, [2014]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 05 jan. 2023.

BRASIL. **Medida Provisória nº 954, de 17 de abril de 2020**. Dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020. Brasília, DF: Presidência da República, [2020]. Disponível em: http://www.planalto.gov.br/CCIVIL_03/_Ato2019-2022/2020/Mpv/mpv954.htm. Acesso em: 14 jan. 2023.

BRASIL. Supremo Tribunal Federal. Julgamento das Medidas Cautelares nas Ações Diretas de Inconstitucionalidade 6387, 6388, 6389, 6390 e 6393. 2020. Disponível em: https://jurisprudencia.stf.jus.br/pages/search?base=acordaos&pesquisa_inteiro_teor=fals

e&sinonimo=true&plural=true&radicais=false&buscaExata=true&page=1&pageSize=10&queryString=ADI%206387&sort=_score&sortBy=desc. Acesso em:20 de mar.2023.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 17 mar. 2023.

CASTELLS, Manuel. **A galáxia da internet**: reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Zahar, 2003.

COMPARATO, Fábio Konder. **A afirmação histórica dos direitos humanos**. 12. ed. São Paulo: Saraiva, 2019.

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.

FROSINI, Tommaso Edoardo. Nuevas tecnologías y constitucionalismo**. Revista Derecho del Estado**, *[S. l.]*, n. 15, p. 29–44, 2003. Disponível em: https://revistas.uexternado.edu.co/index.php/derest/article/view/798. Acesso em: 31 jan. 2023.

LEAL, Rogério Gesta. Direito fundamental à proteção de dados em tempos de pandemia: necessárias equações entre segurança pública e privada. **Revista Brasileira de Direitos Fundamentais & Justiça**, Belo Horizonte, ano 14, n. 43, p. 357-374, jul./dez., 2020

LEAL, Rogério Gesta. **Perspectivas hermenêuticas dos direitos humanos e fundamentais no Brasil**. Porto Alegre: Livraria do Advogado, 2000.

LEAL, Rogério Gesta. **A Responsabilidade penal do patrimônio ilícito como ferramenta de enfrentamento da criminalidade**. Porto Alegre: FMP, 2017, Disponível em http://www.fmp.edu.br/servicos/285/publicacoes/. Acesso em: 13 mar. 2023.

LIMA, Cíntia Rosa Pereira de. **Autoridade Nacional de proteção de dados e a efetividade da Lei Geral de Proteção de Dados**. São Paulo: Almedina, 2020.

MACHADO, Marta Rodriguez de Assis. **Sociedade do Risco e Direito Penal**. Uma avaliação de novas tendências político-criminais. São Paulo: IBCCRIM, 2005.

MENDES, Gilmar Ferreira; FERNANDES, Victor Oliveira. Constitucionalismo digital e jurisdição constitucional: uma agenda de pesquisa para o caso brasileiro. **Revista**

Brasileira de Direito, Passo Fundo, v. 16, n. 1, p. 1-33, out. 2020. ISSN 2238-0604. Disponível em: https://seer.imed.edu.br/index.php/revistadedireito/article/view/4103. Acesso em: 10 jan. 2023. doi:https://doi.org/10.18256/2238-0604.2020.v16i1.4103.

MENDES, Gilmar Ferreira. Os Direitos Fundamentais e seus múltiplos significados na ordem constitucional. **Revista Jurídica Virtual**, Brasília, vol. 2, n. 13, jun. 1999. Disponível em: https://revistajuridica.presidencia.gov.br/index.php/saj/article/view/1011/995 . Acesso em: 15 jan. 2023.

MENDES, Laura Schertel; FONSECA, Gabriel Campos Soares da. STF reconhece direito fundamental à proteção de dados Comentários sobre o referendo da Medida Cautelar nas ADIs 6387, 6388, 6389, 6390 e 6393. **Revista de Direito do Consumidor**, São Paulo, v. 130, p. 471-478, jul./ago. 2020.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Declaração Universal dos Direitos Humanos. 1948. Disponível em https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos. Acesso em: 10 jan. 2023

ORGANIZAÇÃO DOS ESTADOS AMERICANOS. Convenção Americana de Direitos Humanos ("Pacto de San José de Costa Rica"), 1969. Disponível em: https://www.cidh.oas.org/basicos/portugues/c.convencao_americana.htm. Acesso em: 10 jan. 2023.

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

SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. **Curso de Direito Constitucional.** 6. ed. São Paulo: Saraiva, 2017.

SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. 40. ed., rev. e atual. São Paulo: Malheiros, 2017.

SILVEIRA, Alessandra; FROUFE, Pedro. Do mercado interno à cidadania de direitos: a proteção de dados pessoais como a questão jusfundamental identitária dos nossos tempos. **UNIO – *EU Law Journa*l**, vol. 4, No. 2, julho/2018. Disponível em: https://doi.org/10.21814/unio.4.2.2. Acesso em: 5 jan. 2023.

STRECK, Lenio Luiz. **As interceptações Telefônicas e os Direitos Fundamentais**: Constituição, Cidadania, Violência: A lei 9.296/96 e seus reflexos penais e processuais. Porto Alegre: Livraria do Advogado, 1997.

TERRA, Aline de Miranda Valverde; MULHOLLAND, Caitlin. A utilização econômica de rastreadores e identificadores *on-line* de dados pessoais. *In:* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**, São Paulo: Thomson Reuters Brasil, 2019. p. 601-619.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância***:* a luta por um futuro humano na nova fronteira do poder. 1. ed. Rio de Janeiro: Intrínseca, 2020.