XXXI CONGRESSO NACIONAL DO CONPEDI BRASÍLIA - DF

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS III

IRINEU FRANCISCO BARRETO JUNIOR

PAULO CAMPANHA SANTANA

D597
DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS III [Recurso eletrônico on-line] organização CONPEDI
Coordenadores: Irineu Francisco Barreto Junior, Paulo Campanha Santana – Florianópolis: CONPEDI, 2024.
Inclui bibliografia
ISBN: 978-65-5274-063-2
Modo de acesso: www.conpedi.org.br em publicações
Tema: Saúde: UM OLHAR A PARTIR DA INOVAÇÃO E DAS NOVAS TECNOLOGIAS
1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direito. 3. Governança e novas tecnologias.
XXX Congresso Nacional do CONPEDI Fortaleza - Ceará (3: 2024 : Florianópolis, Brasil).
CDU: 34

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

XXXI CONGRESSO NACIONAL DO CONPEDI BRASÍLIA - DF

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS III

Apresentação

O XXXI Congresso do Conselho Nacional de Pesquisa e Pós-Graduação em Direito CONPEDI foi realizado nos dias 27, 28 e 29 de novembro de 2024, em Brasília-DF, e elegeu o tema "Um Olhar a partir da inovação e das novas tecnologias" como eixo norteador dos seus trabalhos. Sob esse escopo, o presente congresso buscou explorar os impactos das inovações tecnológicas no sistema jurídico e nas práticas do Direito, discutindo como as ferramentas digitais estão transformando a pesquisa, a prática profissional e a formação acadêmica na área jurídica.

Saliente-se a enorme aderência entre a temática central do evento e a abordagem do GT Direito, Governança e Novas Tecnologias, um dos mais tradicionais do Conpedi e que, a cada ano, adquire maior centralidade no congresso e no cenário da pesquisa e pós graduação do país. Como de costume o evento propiciou a aproximação entre coordenadores, docentes e pesquisadores de diversos Programas de Pós-Graduação em Direito de todo o Brasil.

A presente edição do Conpedi, dessa forma, abordou o impacto da rápida evolução tecnológica na sociedade, destacando a inovação como essencial para o crescimento e a adaptação em diversos setores. Com foco nas oportunidades geradas por tecnologias como inteligência artificial e big data, especialmente no campo jurídico, o evento também examina os desafios éticos, regulatórios e de acesso que acompanham essas transformações..

Os artigos apresentados GT Direito, Governança e Novas Tecnologias refletem uma ampla diversidade temática que explora as interseções entre tecnologia, direito, ética e sociedade. Diversos artigos destacam o impacto da inteligência artificial (IA) e outras tecnologias emergentes no contexto jurídico, abordando desde a responsabilidade civil e desafios regulatórios até o uso de ferramentas como o ChatGPT na prática jurídica e na proteção de dados pessoais. Destacam-se ainda apresentações exploram os aspectos éticos e econômicos da tecnologia, como biopolítica, biocapitalismo e a monetização de dados pessoais, evidenciando os desafios para a privacidade, integridade corporativa e compliance.

A proteção de direitos fundamentais na era digital, incluindo privacidade, propriedade intelectual e combate à desinformação, também aparece como um tema recorrente. A governança tecnológica é abordada em múltiplas esferas, desde a aplicação de big data na conformidade com a LGPD, até o uso de tecnologia na arrecadação fiscal e no poder

judiciário, com análises institucionais e regulatórias. Em paralelo, pesquisadores analisam o impacto da tecnologia na educação, como a exclusão digital e os desafios para educadores, e a transformação de setores específicos, como a arbitragem desportiva e os ambientes clínicos.

Por fim, destacam-se reflexões sobre democracia digital e participação popular, bem como a valorização do trabalho humano e a relação entre ética algorítmica e integridade corporativa. Esses temas revelam uma preocupação transversal com a construção de uma sociedade tecnológica mais equitativa e ética, com foco na adaptação de instituições e na proteção de direitos em um contexto de acelerada transformação digital.

Os coordenadores responsáveis pelo Grupo de Trabalho cordialmente convidam os interessados a examinar integralmente os artigos em questão, confiantes de que a leitura será proveitosa. Encerramos esta apresentação expressando gratidão pela oportunidade de facilitar os diálogos entre pesquisadores de elevada competência.

Prof. Dr. Irineu Francisco Barreto Junior. Mestrado em Direito da Sociedade da Informação das Faculdades Metropolitanas Unidas - FMU-SP.

Prof. Dr. Paulo Campanha Santana. Mestrado em Direito das Relações Sociais e Trabalhistas do Centro Universitário do Distrito Federal (UDF)

RESPONSABILIDADE CIVIL NA ERA DIGITAL: DESAFIOS JURÍDICOS E IMPLICAÇÕES DAS TECNOLOGIAS EMERGENTES NO BRASIL

CIVIL LIABILITY IN THE DIGITAL AGE: LEGAL CHALLENGES AND IMPLICATIONS OF EMERGING TECHNOLOGIES IN BRAZIL

Tiago Cappi Janini [1]
Ester Soares Moura [2]
Irineu Francisco Barreto Junior [3]

Resumo

No contexto contemporâneo da crescente interação entre humanos e sistemas computacionais, a responsabilidade civil em matéria de informática emerge como uma preocupação central. Diante disso, esta pesquisa como problema: como aplicar o instituto da responsabilidade civil para enfrentar os conflitos sociais decorrentes da intersecção entre direito e tecnologia? Utilizando-se o método dedutivo, a revisão bibliográfica e a análise de casos jurisprudenciais relevantes, este artigo tem por objetivo específico oferecer uma visão sobre como o direito está se adaptando às necessidades impostas pela era digital, de modo a garantir uma proteção efetiva dos direitos dos usuários e a atribuição justa de responsabilidades. Os objetivos gerais são: descrever os marcos regulatórios legais da responsabilidade civil em informática no Brasil; analisar casos emblemáticos acerca da responsabilidade civil no âmbito digital; identificar os desafios da jurídicos da responsabilidade civil na era digital; refletir sobre o microssistema do ambiente digital e responsabilidade civil.

Palavras-chave: Sociedade da informação, Responsabilidade civil, Proteção de dados, Microssistema jurídico do ambiente digital, Tecnologias disruptivas

Abstract/Resumen/Résumé

In the contemporary context of the growing interaction between humans and computer systems, civil liability in information technology matters emerges as a central concern. In view of this, this paper investigates how to apply the institute of civil liability to face the social conflicts arising from the intersection between law and technology? Using the deductive method, the literature review and the analysis of relevant jurisprudential cases, this

[1] Doutor em Direito pela PUC-SP. Professor permanente do Programa de Mestrado em Direito na Sociedade da Informação FMU-SP. Pós-Doutor pela Universidade Estadual do Norte do Paraná (UENP), bolsista PNPD-CAPES.

[2] Mestranda em Direito da Sociedade de Informação pelo Centro Universitário das Faculdades Metropolitanas Unidas – FMU/SP. Professora universitária no curso de Direito pelo Centro Universitário Adventista de São Paulo UNASP

[3] Pós Doutor em Sociologia pela USP e Doutor pela PUC-SP. Docente do Programa de Mestrado em Direito da Sociedade da Informação FMU-SP. Analista de Pesquisas da Fundação Seade-SP.

article has the specific objective identify how the law is adapting to the needs imposed by the digital age, to ensure effective protection of users' rights and the fair attribution of responsibilities. The general objectives are to describe the legal regulatory frameworks for civil liability in information technology in Brazil; analyze emblematic cases on civil liability in the digital sphere; identify the legal challenges of civil liability in the digital age; reflect on the microsystem of the digital environment and civil liability.

Keywords/Palabras-claves/Mots-clés: Information society, Liability, Data protection, Legal microsystem of the digital environment, Disruptive technologies

Introdução

No cenário atual, marcado pela acelerada evolução tecnológica e pela digitalização de inúmeras esferas da atividade humana, a questão da responsabilidade civil em matéria de informática adquire uma relevância sem precedentes. Este artigo, busca explorar a complexa interação entre direito e tecnologia, focando especificamente nas implicações legais emergentes no contexto brasileiro. A responsabilidade civil, tradicionalmente voltada para a compensação de danos através de princípios como a negligência e a responsabilidade objetiva, enfrenta novos desafios quando aplicada ao dinâmico e muitas vezes nebuloso campo da informática.

A ascensão de tecnologias disruptivas — como a inteligência artificial, blockchain, e Internet das Coisas (IoT) — não só transforma a infraestrutura de nossas interações sociais e econômicas, mas também eleva significativamente os riscos de danos que podem ser causados de maneiras até então inimagináveis. Vazamentos de dados pessoais, ataques cibernéticos, e falhas de software são apenas alguns exemplos de incidentes que podem acarretar graves prejuízos materiais e morais para os indivíduos afetados.

O problema que norteia este trabalho consiste na seguinte questão: como aplicar o instituto da responsabilidade civil para enfrentar os conflitos sociais decorrentes da intersecção entre direito e tecnologia?

Utilizando-se do método dedutivo e valendo-se da revisão bibliográfica e análise de casos jurisprudenciais relevantes, este artigo está estruturado para fornecer uma análise detalhada dos marcos regulatórios existentes, como a Lei Geral de Proteção de Dados Pessoais (LGPD) e o Marco Civil da Internet, bem como discutir as lacunas legais que persistem à luz dos desenvolvimentos tecnológicos.

Esta pesquisa tem por objetivo específico oferecer uma visão abrangente sobre como o direito brasileiro está se adaptando às necessidades impostas pela era digital, propondo reflexões sobre possíveis reformas legislativas ou novas interpretações jurídicas que garantam a proteção efetiva dos direitos dos usuários e a atribuição justa de responsabilidades. Os objetivos gerais são: descrever os marcos regulatórios legais da responsabilidade civil em informática no Brasil; analisar casos emblemáticos acerca da responsabilidade civil no âmbito digital; identificar os desafios da jurídicos da responsabilidade civil na era digital; refletir sobre o microssistema do ambiente digital e responsabilidade civil

A meta é contribuir para um framework jurídico que seja tanto robusto quanto flexível, capaz de responder adequadamente às rápidas mudanças do nosso tempo e promover um ambiente digital seguro e justo para todos.

1. Análise Legal da Responsabilidade Civil em Informática: Implicações e Marcos Regulatórios no Brasil

É preciso analisar os aspectos legais e conceituais que sustentam essa área específica do direito. Uma parte essencial dessa análise envolve a revisão das teorias tradicionais de Responsabilidade Civil, como a teoria da negligência e a responsabilidade objetiva, que servem como alicerces para a compreensão das questões jurídicas relacionadas à informática. Ao revisitar as teorias clássicas, busca-se compreender sua adaptação e aplicabilidade aos casos que envolvem tecnologia da informação. Especificamente, investigar como os princípios gerais de Responsabilidade Civil são interpretados e ajustados para se adequarem ao cenário digital em constante evolução. Essa análise permite não apenas entender os fundamentos legais que regem a Responsabilidade Civil em informática, mas também identificar lacunas ou ambiguidades que possam existir na legislação vigente (Agudo, Muchon, 2020).

Além disso, vale investigar as especificidades dos danos que podem surgir como resultado das atividades digitais. Desde violações de dados até a perda de privacidade e os danos econômicos decorrentes de falhas em sistemas informáticos, cada tipo de dano apresenta desafios únicos em termos de atribuição de Responsabilidade Civil e quantificação de danos. Essa análise aprofundada é crucial para uma compreensão abrangente das implicações jurídicas da informática (Bioni; Dias, 2020).

Adicionalmente, a investigação de casos jurisprudenciais relevantes desempenha um papel fundamental na construção do conhecimento sobre a Responsabilidade Civil em informática. Ao examinar como os tribunais têm interpretado e aplicado os princípios de Responsabilidade Civil em casos específicos de informática, será possível obter informações valiosas sobre padrões de decisões judiciais, tendências emergentes e desafios enfrentados na prática jurídica digital.

No Brasil, a Lei Geral de Proteção de Dados (LGPD), em vigor desde 2020, desempenha um papel fundamental na regulamentação da Responsabilidade Civil relacionada à informática, estabelecendo diretrizes para o tratamento de dados pessoais e impondo sanções

em caso de violações. O caso emblemático do vazamento de dados do Facebook, envolvendo a consultoria política Cambridge Analytica, revelou em 2018 a dimensão do descumprimento das normas de proteção de dados pessoais. O incidente expôs informações de cerca de 87 milhões de usuários da rede social, sem o devido consentimento, levantando críticas e investigações em várias jurisdições. Tanto o Facebook quanto a Cambridge Analytica foram alvos de penalidades e processos judiciais, destacando a necessidade urgente de medidas mais rigorosas para proteger a privacidade dos usuários.

De acordo com a LGPD, em especial o Artigo 42, a empresa que descumprir as normas de proteção de dados pode ser responsabilizada, sendo aplicável a teoria da responsabilidade objetiva. Conforme estabelecido no Artigo 37 da mesma lei, basta a comprovação do dano e do nexo causal para a responsabilização da empresa, independentemente de culpa, tornando-a responsável pelos danos causados pela violação da proteção de dados pessoais. Assim, a LGPD estabelece diretrizes claras para a responsabilização das empresas em casos de violações, promovendo a proteção dos direitos dos titulares de dados pessoais no contexto digital.

O Marco Civil da Internet (Lei nº 12.965/2014) representa um marco regulatório para a internet no Brasil, estabelecendo princípios, garantias, direitos e deveres para o uso da rede no país. Em relação à proteção de dados, o Marco Civil contém disposições que tangenciam diretamente esse tema, apesar de não ser uma legislação específica. Entre os princípios estabelecidos pelo Marco Civil da Internet, está a proteção da privacidade dos usuários e o respeito à liberdade de expressão, o que está intrinsecamente ligado à segurança dos dados pessoais na rede. Além disso, o Marco Civil estabelece diretrizes para a atuação dos provedores de serviços na internet, como provedores de acesso e aplicações online, exigindo transparência nas políticas de privacidade e na coleta, armazenamento e tratamento de dados pessoais dos usuários.

O Código de Defesa do Consumidor (Lei nº 8.078/1990) representa um dos pilares do ordenamento jurídico brasileiro, assegurando direitos fundamentais aos consumidores em diversas esferas de suas relações comerciais. Embora sua principal finalidade seja resguardar os interesses dos consumidores em transações comerciais, suas disposições também abrangem questões relacionadas à proteção de dados pessoais. Nesse sentido, embora não tenha sido elaborado especificamente para tratar dessa temática, o CDC estabelece um arcabouço legal que pode ser aplicado em casos de violações de dados que afetem os consumidores.

Ao garantir a proteção dos consumidores contra práticas abusivas e lesivas por parte das empresas, o CDC contribui para a responsabilização das organizações que negligenciam a

segurança e privacidade dos dados pessoais de seus clientes. Por meio de suas disposições sobre responsabilidade objetiva e solidária, o código estabelece que as empresas são responsáveis por danos causados aos consumidores em decorrência de falhas na proteção de dados, independentemente de culpa. Isso significa que, ao ocorrer uma violação de dados que resulte em prejuízos para os consumidores, as empresas podem ser responsabilizadas e obrigadas a reparar os danos causados.

O Código Civil Brasileiro (Lei nº 10.406/2002) representa outro pilar do ordenamento jurídico brasileiro, abrangendo diversas áreas do direito civil e estabelecendo os fundamentos legais para as relações interpessoais na sociedade. Dentro desse contexto abrangente, esse Código se aplica na proteção da privacidade e dos dados pessoais dos cidadãos. Embora não seja uma legislação específica voltada para a proteção de dados, suas disposições são aplicáveis em situações que envolvem violações dessa natureza. Especificamente, o Código Civil estabelece preceitos que respaldam a proteção da privacidade e dos dados pessoais, especialmente quando essas violações resultam em danos morais e materiais para os indivíduos afetados. Ao reconhecer a importância da integridade e da inviolabilidade das informações pessoais, o código oferece ferramentas legais para que as vítimas possam buscar reparação pelos prejuízos sofridos em decorrência de violações de dados.

Assim, em situações em que a violação de dados pessoais acarreta danos às vítimas, o Código Civil pode ser invocado para responsabilizar os responsáveis e garantir que as medidas necessárias sejam tomadas para reparar os danos causados. Dessa forma, o Código Civil desempenha um papel complementar às legislações específicas de proteção de dados, contribuindo para a construção de um ambiente jurídico que promova a segurança e a privacidade dos dados pessoais dos cidadãos brasileiros.

É importante ressaltar o papel fundamental do Estatuto da Criança e do Adolescente (Lei nº 8.069/1990) na garantia da proteção integral dos direitos das crianças e adolescentes no Brasil. Este estatuto não apenas estabelece medidas de proteção específicas para essa parcela da população, mas também reconhece a importância da privacidade e da segurança dos dados pessoais desses indivíduos em um mundo cada vez mais digitalizado. Ao considerar a vulnerabilidade peculiar das crianças e adolescentes, o Estatuto da Criança e do Adolescente inclui disposições que visam assegurar a proteção de suas informações pessoais. Essas disposições abrangem desde a coleta e o tratamento de dados até a sua utilização em contextos diversos, como em ambientes escolares, serviços de saúde e nas relações familiares e sociais.

Ao abordar a proteção de dados no contexto da infância e adolescência, o Estatuto da Criança e do Adolescente complementa o arcabouço legal existente, reconhecendo a necessidade de medidas específicas para garantir a segurança e a privacidade das informações pessoais desses indivíduos em conformidade com os princípios estabelecidos pela legislação nacional e internacional de proteção de dados. Em suma, o Estatuto da Criança e do Adolescente contribui para a promoção de um ambiente seguro e saudável para o desenvolvimento das futuras gerações, onde a proteção dos dados pessoais desempenha um papel cada vez mais relevante.

2. Desafios Jurídicos na Era Digital: Responsabilidade Civil em Tecnologias Emergentes e Casos Precedentes

Inúmeros desafios jurídicos derivam da nova era denominada Sociedade da Informação, na qual tecnologias como Inteligência Artificial são treinadas usando gigantescos volume de dados (Barreto Junior; Molina, 2022, p. 245). Somam-se às determinações da LGPD quanto à tutela de dados pessoais sensíveis e a autodeterminação informativa (Barreto Junior; Naspolini, 2019, p. 140)

Nesse contexto, o advento de tecnologias como inteligência artificial, blockchain e Internet das Coisas tem transformado profundamente a maneira como os sistemas computacionais são desenvolvidos e utilizados. A inteligência artificial capacita os sistemas a realizarem tarefas que normalmente exigiriam intervenção humana, enquanto o blockchain estabelece um registro imutável e transparente de transações e a Internet das Coisas interconecta dispositivos físicos para coletar e trocar dados. Essas tecnologias têm um impacto profundo na sociedade, transformando a maneira como as pessoas vivem, trabalham e se relacionam. No entanto, junto com os benefícios, surgem desafios únicos para o quadro jurídico existente, incluindo questões sobre responsabilidade por decisões algorítmicas, segurança e privacidade de dados, bem como desafios relacionados à regulamentação e governança dessas tecnologias em constante evolução. Portanto, o avanço dessas tecnologias exige uma revisão e adaptação contínuas do sistema legal para garantir que os direitos individuais e coletivos sejam protegidos de forma adequada (Figueiredo, 2024).

Uma das questões centrais é a atribuição de responsabilidade por decisões algorítmicas. Com o aumento da automação e da tomada de decisões baseadas em algoritmos,

surgem dilemas éticos e legais sobre quem é responsável por eventuais danos causados por sistemas autônomos. A falta de transparência em algoritmos complexos e a possibilidade de viés algorítmico destacam a necessidade de revisão das normas de Responsabilidade Civil para garantir uma distribuição justa e equitativa de responsabilidades (Téffe; Medon, 2019)

A segurança cibernética se tornou uma preocupação com o aumento de ataques cibernéticos e violações de dados. A Responsabilidade Civil em casos de violações de segurança levanta questões sobre a diligência das empresas na proteção de informações confidenciais e a compensação adequada às vítimas de tais incidentes. Com a natureza transnacional da internet, surgem desafios adicionais na determinação da jurisdição competente e na aplicação de leis de Responsabilidade Civil em casos que envolvem partes localizadas em diferentes países. A análise das práticas de cooperação internacional e dos esforços para harmonizar leis e regulamentos em nível global será vital para entender como lidar com esses desafios de forma eficaz (Martins, 2020).

Cita-se a ocorrência da Equifax em 2017, onde a empresa de relatórios de crédito sofreu uma violação de segurança maciça que expôs os dados sensíveis de milhões de pessoas. Os tribunais nesse caso tiveram que determinar se a Equifax agiu com a diligência necessária na proteção desses dados e se deveria ser responsabilizada pelos danos resultantes da violação. A decisão judicial não apenas considerou a gravidade da violação, mas também avaliou as medidas de segurança implementadas pela empresa e sua resposta ao incidente. A empresa enfrentou várias ações judiciais nos Estados Unidos. Um dos desdobramentos mais significativos foi um acordo firmado em 2019 entre a Equifax e várias agências reguladoras federais e estaduais dos EUA. Sob este acordo, a Equifax concordou em pagar uma multa de cerca de US$ 700 milhões e estabelecer um fundo de compensação para as vítimas afetadas pela violação. A decisão judicial considerou que a citada falhou em proteger adequadamente os dados dos consumidores e que a empresa deveria ser responsabilizada por danos financeiros e pessoais resultantes da violação.

Outro exemplo relevante é o caso "Google Street View Wi-Fi Sniffing", no qual o Google foi processado por coletar ilegalmente dados de redes Wi-Fi domésticas durante a operação de seus veículos Street View. Os tribunais analisaram se essa coleta de dados constituía uma violação de privacidade e se o Google deveria ser responsabilizado por danos resultantes da violação. Em 2013, o Google concordou em pagar uma multa de US$ 7 milhões para encerrar uma investigação conduzida por procuradores-gerais de 38 estados dos EUA devido à coleta ilegal de dados de redes Wi-Fi domésticas durante as operações do Google

Street View. Além disso, a empresa também concordou em implementar medidas adicionais de privacidade e segurança de dados. A decisão judicial considerou que a coleta de dados Wi-Fi pelo Google sem consentimento adequado constituía uma violação de privacidade e que a empresa deveria ser responsabilizada por essas ações.

Esses casos demonstram como a jurisprudência em matéria de informática considera questões complexas relacionadas à segurança de dados, privacidade e responsabilidade das empresas, ajudando a estabelecer padrões legais e éticos para o uso da tecnologia da informação.

3. Responsabilidade Civil na Era Digital: Desafios e Perspectivas na Era da Informação

A teoria da negligência e a responsabilidade objetiva são conceitos fundamentais no âmbito da Responsabilidade Civil em matéria de informática, onde a dinâmica das relações jurídicas é intrinsecamente ligada à tecnologia. A teoria da negligência, nesse contexto, refere-se à conduta imprudente ou descuidada que causa danos a terceiros no uso de sistemas ou serviços digitais. Por exemplo, se uma empresa não implementa medidas de segurança adequadas em seu sistema de armazenamento de dados e ocorre um vazamento de informações sensíveis dos clientes devido a essa falha, essa empresa pode ser considerada negligente (Bernardino, 2022).

Por outro lado, a responsabilidade objetiva se baseia na ideia de que determinadas atividades ou produtos são intrinsecamente arriscados, independentemente do nível de cuidado exercido pelo responsável. Na esfera da informática, isso pode ser aplicado quando um produto ou serviço digital falha independentemente de quaisquer precauções tomadas. Se um software apresenta um bug que resulta na perda de dados do usuário, mesmo que a empresa tenha agido com diligência na sua criação, ela pode ser responsabilizada objetivamente pelos danos causados (Bernadino, 2022).

As teorias da negligência e da responsabilidade objetiva em matéria de informática estão intrinsecamente relacionadas aos princípios e garantias fundamentais estabelecidos na Constituição Federal Brasileira. Em primeiro lugar, é importante considerar os direitos fundamentais consagrados na Constituição, tais como o direito à privacidade e à proteção de dados pessoais. A negligência na segurança dos sistemas digitais pode violar esses direitos, e a responsabilidade objetiva pode ser empregada para assegurar a devida compensação às vítimas

de tais violações, preservando, assim, a dignidade da pessoa humana, um princípio basilar da Constituição (Brasil, 1988; Bernadino, 2022).

O direito à segurança, garantido pela Constituição, abrange o ambiente digital. A falta de cuidado na proteção de dados ou na implementação de medidas de segurança adequadas pode infringir esse direito. Nesse sentido, a responsabilidade objetiva pode ser evocada para garantir que os agentes sejam responsabilizados pela ausência de segurança nos sistemas e serviços digitais, contribuindo para a preservação da integridade e da segurança dos cidadãos no ambiente virtual (Brasil, 1988).

Lawrence Lessig, renomado professor de direito na Universidade de Harvard e uma figura proeminente no campo do direito digital. Em suas obras, como "Code: And Other Laws of Cyberspace", Lessig (2009) explora a interação complexa entre tecnologia e legislação. Ele argumenta que o código, ou seja, o software que governa os sistemas digitais, pode ter um papel semelhante ao da lei na regulamentação do comportamento online. Lessig adverte contra a negligência na codificação de sistemas, destacando como falhas de segurança podem resultar em implicações legais significativas.

Jonathan Zittrain (2008), um dos principais especialistas em direito da internet e segurança cibernética, com influência global, professor em Harvard e co-fundador do Berkman Klein Center, analisa as questões emergentes em sistemas tecnológicos, como governança da internet, neutralidade da rede e criptografia. Sua obra "The Future of the Internet and How to Stop It" examina os desafios da era digital, propondo soluções para promover a inovação e proteger os direitos individuais. Zittrain é frequentemente chamado para aconselhar governos e organizações internacionais, sendo uma figura central na defesa da internet como um espaço livre, aberto e seguro. Seus prêmios e honrarias reconhecem seu trabalho visionário em moldar o futuro da internet para todos.

Richard A. Epstein é reconhecido por suas valiosas contribuições para a teoria jurídica, concentrando-se principalmente no direito privado e questões relacionadas à propriedade. Seus escritos oferecem percepções relevantes sobre a Responsabilidade Civil em ambientes tecnológicos, examinando a aplicação das teorias da negligência e da responsabilidade objetiva nesses contextos específicos. Em obras como *"Takings: Private Property and the Power of Eminent Domain"*, Epstein (1986) investiga como o direito tradicional pode ser ajustado para enfrentar os desafios legais decorrentes do avanço tecnológico. Essa análise profunda e meticulosa oferece perspectivas cruciais para lidar com as complexidades legais emergentes no cenário da tecnologia moderna.

Bruce Schneier, por sua vez, é um especialista em segurança cibernética amplamente reconhecido, cujo trabalho influencia tanto a academia quanto a prática na área. Schneier (2012) examina como a segurança digital se relaciona com questões de responsabilidade e negligência. Em obras como *"Liars and Outliers: Enabling the Trust that Society Needs to Thrive"*, destaca a importância de políticas de segurança robustas e defende a responsabilização dos fabricantes de software e hardware por falhas de segurança.

Esses autores representam uma gama diversificada de perspectivas sobre as questões legais e éticas relacionadas à tecnologia, oferecendo análises críticas e propostas para abordar os desafios emergentes na sociedade digital. Suas contribuições são fundamentais para informar o debate sobre responsabilidade em matéria de informática e moldar políticas que garantam a segurança e proteção dos usuários e suas informações pessoais.

Apesar dos esforços para responsabilizar os indivíduos e empresas envolvidos em questões de informática, ainda existem lacunas significativas na legislação. Uma das principais lacunas está relacionada à falta de clareza e especificidade nas leis existentes, que muitas vezes não acompanham o ritmo das mudanças tecnológicas. Isso pode levar a interpretações ambíguas e inconsistências na aplicação da lei, dificultando a responsabilização efetiva dos culpados e a proteção dos direitos das vítimas (Meireles 2020).

Por exemplo, embora a LGPD estipule que as empresas são responsáveis por proteger os dados pessoais dos usuários, não há uma definição precisa sobre quem seria responsável em caso de vazamento de dados devido a falhas de segurança. Isso pode levar a interpretações divergentes e inconsistências na aplicação da lei pelos tribunais, dificultando a responsabilização efetiva dos culpados e a proteção dos direitos das vítimas (Brasil, 2018).

Embora o CDC brasileiro seja uma lei abrangente que estabelece os direitos dos consumidores em várias áreas, incluindo transações comerciais online, sua aplicação específica em casos de problemas relacionados à informática pode ser desafiadora. As disposições do CDC não abordam adequadamente questões como vazamentos de dados, fraudes online e danos decorrentes de falhas em sistemas de tecnologia da informação. A falta de atualização do CDC para contemplar essas questões específicas deixa lacunas na proteção dos consumidores em um ambiente digital em constante evolução (Brasil, 1990).

Embora muitos países tenham leis específicas para crimes cibernéticos, como a Lei de Crimes Cibernéticos nos Estados Unidos e a Lei de Segurança Cibernética no Reino Unido, essas legislações podem enfrentar dificuldades em manter-se atualizadas com as táticas em

constante mudança dos criminosos digitais. Muitas vezes, essas leis carecem de detalhes específicos sobre responsabilidades legais em casos de cibercrimes, especialmente quando se trata de determinar quem é responsável por ataques sofisticados, como ransomware (um tipo de malware que criptografa os arquivos das vítimas, exigindo um resgate para desbloqueá-los) ou *phishing* (uma técnica de engenharia social usada para induzir os usuários a fornecerem informações confidenciais, como senhas e informações financeiras) (Meireles 2020).

Por exemplo, a Lei de Crimes Cibernéticos dos Estados Unidos não fornece orientações claras sobre como responsabilizar as partes envolvidas em ataques cibernéticos complexos, como aqueles que envolvem múltiplos atores e jurisdições. Da mesma forma, a Lei de Segurança Cibernética no Reino Unido, embora aborde questões como acesso não autorizado a sistemas de computador, não oferece diretrizes específicas sobre responsabilidade em casos de ataques de *phishing* que resultam em roubo de dados pessoais.

No contexto brasileiro, apesar da existência do Marco Civil da Internet e da LGPD, ainda há desafios significativos relacionados à responsabilização em casos de cibercrimes como *ransomware ou phishing*. Embora essas leis forneçam uma base legal para lidar com questões de segurança cibernética e proteção de dados, a aplicação específica em situações de ataques cibernéticos sofisticados é insuficiente. A falta de disposições claras e detalhadas sobre Responsabilidade Civil em casos de violações de segurança cibernética deixa lacunas que dificultam a identificação e punição dos responsáveis por tais crimes.

O Marco Civil da Internet estabelece princípios fundamentais para a utilização da internet no Brasil, como a garantia da privacidade dos usuários e a responsabilidade das empresas pelo armazenamento de dados pessoais. No entanto, a lei carece de especificidades sobre como responsabilizar os agentes envolvidos em ataques cibernéticos, especialmente aqueles envolvendo ransomware, onde os responsáveis muitas vezes estão localizados em jurisdições estrangeiras.

Da mesma forma, a LGPD estabelece regras para o tratamento de dados pessoais, incluindo medidas de segurança para proteger essas informações contra acessos não autorizados. No entanto, a lei não aborda diretamente a Responsabilidade Civil em casos de violações de dados decorrentes de ataques cibernéticos, como no caso do phishing, onde informações confidenciais são obtidas por meio de engenharia social.

A colaboração entre as legislações nacionais e internacionais referentes à Responsabilidade Civil em assuntos de informática é altamente relevante. Tratados como a

Convenção de Budapeste sobre Cibercrime estabelecem diretrizes comuns para enfrentar crimes cibernéticos, incluindo disposições sobre responsabilidade penal e cooperação entre fronteiras. Organizações como Interpol e Europol facilitam a coordenação entre autoridades policiais de diversos países para investigar e combater crimes cibernéticos, muitos dos quais têm implicações em termos de Responsabilidade Civil. Além disso, regulamentações como o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia têm impacto global, influenciando países como o Brasil a fortalecer suas próprias leis de proteção de dados para estar em conformidade com os padrões internacionais (Brito, 2014).

4. Responsabilidade Civil sob a perspectiva do Microssistema Jurídico no Ambiente Digital

No final do século XIX, há uma ruptura da visão monolítica dos códigos como o eixo central do ordenamento normativo, originado um corpo legislativo fragmentado com uma pluralidade de estatutos autônomos, que além de regularem um assunto específico de forma exaustiva, trazem os princípios, valores e critérios para sua devida interpretação, sob a força normativa do texto constitucional. A lei especial deixa de ser um mero complemento das normas codificadas para possuir autonomia, com princípios e institutos específicos, aglutinando normas de distintos ramos do direito. Aparecem os microssistemas.

Tepedino (2000, p. 11) elucida a necessidade de uma nova composição do ordenamento jurídico:

> O legislador contemporâneo, instado a compor, de maneira harmônica, o complexo de fontes normativas, formais e informais, nacionais e supranacionais, codificadas e extracodificadas, deve valer-se de prescrições narrativas e analíticas, em que consagra expressamente critérios interpretativos, valores a serem preservados, princípios fundamentais como enquadramentos axiológicos com teor normativo e eficácia imediata, de tal modo que todas as demais regras do sistema, respeitados os diversos patamares hierárquicos, sejam interpretadas e aplicadas de maneira homogênea e segundo conteúdo objetivamente definido.

Observando-se a presença dos microssistemas no ordenamento jurídico nacional, em conjunto com o reconhecimento do ambiente digital como lugar de realização de condutas sociais que demandam uma atuação do direito, identifica-se “[...] um cenário que reclama pela

identificação de um microssistema para a proteção de dados e utilização da inteligência artificial" (Macedo *et. al*., 2023, p. 08).

Nesse passo, há elementos suficientes que permitem a identificação de um microssistema jurídico que tutele os cidadãos em suas interações no âmbito digital. Tem-se denominado "microssistema jurídico do ambiente digital" aquele que versa acerca da proteção de dados e os limites da aplicação das novas tecnologias na sociedade, com fins de preservar os direitos fundamentais e humanos.

As relações sociais que passam a ser concretizadas no ambiente digital irritam o sistema jurídico. Surgem conflitos que necessitam de soluções impostas pelo direito. Foi o que aconteceu com o crime de exposição de imagens pornográficas envolvendo criança ou adolescente. A prática desse crime no ciberespaço movimento as estruturas do direito e inclui-se dispositivos no Estatuto da Criança e do Adolescente criminalizando a prática no ciberespaço. Com isso, "O microssistema jurídico do ambiente digital, em uma acepção ampla, se preocupa em proporcionar uma estrutura digital confiável, eficiente e legítima, com principiologia e os institutos próprios que o atual contexto sociojurídico reivindica, oferecendo respostas às demandas públicas e privadas da Sociedade da Informação". (Janini, 2023, p. 147).

O microssistema jurídico do ambiente digital reclama uma constante interação e interpretação das diversas fontes normativas que regulam as condutas conflituosas no ciberespaço. Os idealizadores (Macedo *et al.*, 2023, p. 17) dessa estrutura esclarecem:

> A construção doutrinária que se propõe entende, portanto, que a proteção de dados pessoais não está restrita à Lei Geral de Proteção de Dados. Em verdade, a exegese deve ir ao encontro de se estabelecer um diálogo com outras fontes normativas compatíveis, a fim de relacionar a legislação à luz de vetores coerentes e complementares para conformá-la à realidade e aos direitos fundamentais.

A proposta de construção de um microssistema do ambiente digital torna-se importante instrumento para enfrentar as dificuldades encontradas em termos de responsabilidade civil diante das novas tecnologias, como os casos de danos causados pela Inteligência Artifial (Fujita, 2023). Em interessante debate apresentado por Nivaldo Vícola (2023) sobre a responsabilidade em situações que resultem de acidentes que envolverem automóveis autônomos direciona para a importância do microssistema como forma de resolver essas demandas, por inexistir norma jurídica específica sobre o tema no direito brasileiro.

A proposta do microssistema digital permite a identificação de normas que versam diretamente sobre temas essenciais para a sociedade da informação que se interrelacionem com

direta ou indiretamente com a proteção de dados, como são as situações envolvendo a responsabilidade civil diante das novas tecnologias.

Conclusão

A análise da Responsabilidade Civil em informática no Brasil revela um panorama multifacetado, permeado por desafios dinâmicos e em constante evolução. Embora as leis existentes, como a LGPD, o Marco Civil da Internet e o CDC, forneçam uma base legal para lidar com as crescentes questões de segurança cibernética, proteção de dados e direitos dos consumidores no cenário digital, ainda há lacunas significativas que clamam por soluções mais robustas.

Uma das principais dificuldades enfrentadas reside na falta de clareza e especificidade nas leis vigentes. Frequentemente, essas leis não conseguem acompanhar o ritmo vertiginoso das mudanças tecnológicas, resultando em interpretações ambíguas e inconsistências na sua aplicação. A rápida evolução do panorama digital também expõe lacunas na proteção dos consumidores. Embora o CDC seja abrangente em muitos aspectos, sua aplicabilidade nem sempre é adequada para questões específicas, como vazamentos de dados e fraudes online, que se tornaram cada vez mais comuns.

As leis existentes enfrentam desafios em manter-se atualizadas diante das táticas em constante mutação dos criminosos digitais. Os avanços na tecnologia muitas vezes superam a capacidade das leis de crimes cibernéticos em acompanhar e combater eficazmente as novas formas de ataques. Especialmente preocupante é a falta de disposições claras sobre a responsabilidade em casos de ataques cibernéticos sofisticados, como ransomware ou phishing, que podem causar danos significativos a empresas e indivíduos.

Diante desses desafios, uma série de recomendações se apresenta como essencial para fortalecer o sistema normativo e promover um ambiente digital mais seguro. Em primeiro lugar, urge a necessidade de atualizar as leis existentes para contemplar as especificidades do ambiente digital, garantindo que sejam flexíveis o suficiente para acompanhar os avanços tecnológicos. Além disso, a criação de leis específicas para crimes cibernéticos, definindo claramente responsabilidades e penalidades, é indispensável para dissuadir e punir os perpetradores desses delitos.

Paralelamente, vale promover uma cultura de segurança cibernética, investindo em educação e conscientização para mitigar os riscos associados às atividades digitais. A disseminação de boas práticas e medidas de proteção pode empoderar os usuários a se protegerem contra ameaças online e contribuir para a redução da incidência de crimes cibernéticos. Além disso, o fortalecimento da cooperação internacional é fundamental para enfrentar os desafios que transcendem as fronteiras nacionais, garantindo uma resposta coordenada e eficaz diante das ameaças digitais globais.

REFERÊNCIAS

AGUDO, Hugo Crivilim; MUCHON, Beatriz Vieira. Análise da responsabilidade civil na era tecnológica. **Braz. J. deDevelop**., Curitiba, v. 7, pág.43773-43787, julho.2020.

BARRETO JUNIOR, Irineu Francisco; NASPOLINI, Samyra Haydêe Dal Farra. Proteção de informações no mundo virtual: a LGPD e a determinação de consentimento do titular para tratamento de dados pessoais. **Cadernos Adenauer XX** (2019), nº3 Proteção de dados pessoais: privacidade versus avanço tecnológico Rio de Janeiro: Fundação Konrad Adenauer, outubro 2019.

BARRETO JUNIOR, Irineu Francisco; MOLINA, Fernanda Zampieri. (2022). Capitalismo de plataforma: a ameaça ao direito à autodeterminação informativa na Sociedade da Informação. **Revista Brasileira De Estudos Políticos**, 125, jul./dez. 2022. Disponível em: https://pos.direito.ufmg.br/rbep/index.php/rbep/article/view/852/657. Acesso em 19 ago. 2024.

BERNARDINO, Laura. **Responsabilidade Civil no Direito Digital**. Disponível em: https://www.jusbrasil.com.br/artigos/responsabilidade-civil-no-direito-digital/1571768418. Acesso em 01 abr. 2024.

BIONI, Bruno; DIAS, Daniel. Responsabilidade Civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. **civilistica.com**, a. 9, n. 3, 2020.

BRASIL. **Constituição Federal de 1988**. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 01 04 2024.

BRASIL. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 25 mar. 2024.

BRASIL. **Lei nº 8.069, de 13 de julho de 1990**. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em 01 abr. 2024.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em 01 abr. 2024.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em 01 abr. 2024.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 01 abr. 2024.

BRITO, Adriane. **O regime internacional da internet**: construções argumentativas sobre sua especialidade. São Paulo, 2014. Dissertação de Mestrado, Universidade de São Paulo.

EPSTEIN, Richard A. **Takings**: Private Property and the Power of Eminent Domain. Cambridge, Massachusetts: Harvard University, 1985.

EUROPEAN COMMISSION. **Regulamento Geral sobre a Proteção de Dados**. Disponível em: https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_pt. Acesso em 01 abr. 2024.

FIGUEIREDO, Flávia. **O futuro do Direito Digital**: tendências e perspectivas. Disponível em: https://direitoemconformidade.com.br/2024/02/07/o-futuro-do-direito-digital-tendencias-e-perspectivas-2/. Acesso em 01 abr. 2024.

FUJITA, Jorge Shiguemitsu. Responsabilidade civil no microssistema. *In*: VIGLIAR, José Marcelo Menezes (Org.). **Microssistema jurídico do ambiente digital**. 2. ed. São Paulo: Editora dos Autores, 2023, p. 101-112.

GODINHO, Adriano Marteleto; BONNA, Alexandre Pereira; NERY, Ana Rita de Figueiredo; MIRAGEM Bruno. **Responsabilidade Civil e novas tecnologias**. Indaiatuba-SP: Editora Foco, 2020.

GONÇALVES, Kamila; REGATTIERI, Silvia Maria Alvim. Tecnologia e cultura: entendendo as relações sociais na era digital. **Interface Tecnológica**, 2017.

JANINI, Tiago Cappi. Administração Pública no microssistema jurídico do ambiente digital. *In*: VIGLIAR, José Marcelo Menezes (Org.). **Microssistema jurídico do ambiente digital**. 2. ed. São Paulo: Editora dos Autores, 2023, p. 144-156.

LESSIG, Lawrence. **Code**: And Other Laws of Cyberspace. ReadHowYouWant.com, 2009

MACEDO, Caio Sperandeo, *et. al*. **Microssistema jurídico do ambiente digital**. 1. ed. São Paulo: Ed. dos Autores, 2023.

MARTINS, Amanda Cunha e Mello Smith. **A segurança cibernética levanta questões sobre a Responsabilidade Civil das empresas na proteção de dados, envolvendo desafios como determinação de jurisdição transnacional e cooperação internacional para harmonização regulatória.** São Paulo, 2020. Dissertação de Mestrado, Universidade de São Paulo.

MEIRELES, Julia. **Crimes virtuais e as dificuldades de combatê-los**. Disponível em: https://www.jusbrasil.com.br/artigos/crimes-virtuais-e-as-dificuldades-de-combate-los/876548834. Acesso em 01 abr. 2024.

SCHNEIER, Bruce. **Liars and Outliers**: Enabling the Trust that Society Needs to Thrive. Capa dura – Ilustrado, 14 de fevereiro de 2012.

TÉFFE, Chiara Spadaccini de; Medon Filipe. Responsabilidade Civil e regulação de novas tecnologias: questões acerca da utilização de Inteligência Artificial na tomada de decisões empresariais. **Revista Estudos Institucionais**, v. 6, n. 1, p. 301-333, jan./abr. 2020.

TEPEDINO, Gustavo. O Código civil, os chamados microssistemas e a Constituição: premissas para uma reforma legislativa. *In*: TEPEDINO, Gustavo (coord.). **Problemas de direito civil-constitucional**. Rio de Janeiro: Renovar, 2000. p. 1-16.

VICOLA, Nivaldo Sebastião. A responsabilidade por danos provocados por sistemas de inteligência artificial à luz do Projeto de Lei n. 2338/2023. *In*: VIGLIAR, José Marcelo Menezes (Org.). **Microssistema jurídico do ambiente digital**. 2. ed. São Paulo: Editora dos Autores, 2023, p. 123-143

ZITTRAIN, Jonathan. L. **The Future of the Internet and How to Stop It**. New Haven & London: Yale University Press, 2008.