

PLATAFORMAS DIGITAIS E OS DESAFIOS LEGAIS: EXPLORANDO OS LIMITES DA TERRITORIALIDADE

Gustavo Henrique Bomfim de Carvalho¹

Ronaldo Fenelon Santos Filho²

<https://doi.org/10.55839/2358-7008RCDv12n1pa136-152>

RESUMO

Com o avanço tecnológico das plataformas digitais, somado com o advento das redes sociais, torna-se absolutamente inadiável a discussão a respeito dos impactos que essas inovações podem trazer para a humanidade. Frente a um cenário onde a conectividade transcende as fronteiras físicas, surgem desafios significativos para a aplicação efetiva da Lei. Um dos principais obstáculos enfrentados pelas autoridades legais é a definição dos limites da territorialidade no meio digital. Enquanto o sistema de leis tradicionais é baseado em fronteiras geográficas, as plataformas digitais operam em um espaço virtual que ultrapassam essas delimitações. No Brasil, a implementação da Lei nº 12.965 de 23 de abril de 2014 (Marco Civil da internet), trouxe diversos avanços na regulamentação do uso da internet no país, incluindo princípios como a Neutralidade da rede, a proteção da privacidade dos usuários e a garantia da liberdade de expressão online. No entanto, como qualquer outra legislação, estão embutidos desafios e problemas em sua aplicabilidade como ambiguidade e lacunas, conflitos com outras legislações e principalmente desafios de fiscalização e monitoramento.

Palavras-chaves: Plataformas digitais. Territorialidade. Aplicabilidade. Redes sociais. Lei 12.965/14.

ABSTRACT

¹ Graduando em Direito pela UNAERP. E-mail: rfsantos@unaerp.br

² Possui graduação em Direito pelo Centro Universitário da Fundação Educacional de Barretos (2001) e mestrado em Direito pela Universidade de Ribeirão Preto (2005). Doutor em Direito pela Universidade de Ribeirão Preto (2019). Coordenador do curso de Pós-graduação em direito corporativo e compliance na Escola Paulista de Direito - EPD. É professor titular na UNAERP e professor dos cursos de pós-graduação da Faculdade de Direito de Franca e da EPD. Autor de obras jurídicas e artigos científicos. Atuou como Head Jurídico corporativo em empresas multinacionais e de grande porte. Tem notória experiência nas áreas de Direito Público e Privado. Certificado para atuar como data protection officer (DPO) pelo EXIN - Essentials - Lei Geral de Proteção de Dados (LGPD). Coordenador dos cursos de gestão em serviços jurídicos e notariais, investigação e perícia judicial e segurança privada do Centro Universitário Dom Bosco. E-mail: rfsantos@unaerp.br

With the technological advancement of digital platforms, combined with the advent of Social Media, the discussion regarding the impacts that those innovations can bring to humanity becomes absolutely unavoidable. Faced with a scenario where connectivity transcends physical borders, significant challenges arise for the effective application of the Law. One of the main obstacles faced by legal authorities is defining the limits of Territoriality in the digital area. While the traditional legal system is based on geographical boundaries, digital platforms operate in a virtual space that transcends these geographical limitations. In Brazil, the implementation of Law number 12,965 of April 23, 2014 (Internet Civil Rights Framework) brought several advances in regulating the use of the internet in the country, including principles such as: net neutrality, protection and privacy of users, and freedom of online expression. However, regarding any other legislation, challenges and problems are embedded in its applicability, such as ambiguity, gaps, conflicts with other laws, and primarily challenges of enforcement and monitoring.

Keywords: digital platforms, territoriality, applicability, social media, law 12,965, 2014.

1. INTRODUÇÃO

O rápido desenvolvimento das tecnologias de informações e comunicações, transformou de maneira inconvertível as estruturas das sociedades globais. Com o surgimento das plataformas digitais e a expansão das redes sociais, surgiram novas formas de relações sociais, econômicas e políticas que ultrapassam as fronteiras físicas tradicionais. Essa evolução trouxe consigo uma vasta gama de desafios jurídicos significativos, especificamente no que tange às aplicações e efetividades das leis existentes. No âmbito onde a conectividade não conhece limites geográficos, concerne de maneira imperativa revisitar as bases do direito da Territorialidade para enquadrar à realidade virtual que molda as relações contemporâneas.

Um dos principais desafios enfrentados pelas autoridades legais é a definição e aplicação da territorialidade no âmbito digital. As legislações existentes, demarcadas sob a premissa de fronteira geográficas claramente definidas, confrontam com o espaço virtual, onde tais delimitações são, por sua natureza, fluidas e permeáveis. A lei nº 12.965, de 23 de abril de 2014, conhecida como Marco Civil da Internet no Brasil, representou um avanço significativo ao instituir um conjunto de diretrizes para regular o uso da internet, abrangendo princípios como a neutralidade da rede, a proteção da privacidade dos usuários e a garantia da liberdade de expressão online. No entanto, como analisado em diversas jurisdições ao redor do mundo, tais padronizações enfrentam desafios práticos em sua aplicação, evidenciando a ambiguidade, as

lacunas existentes, os conflitos com outras legislações e as dificuldades relacionadas às fiscalizações e monitoramentos.

Diante ao contínuo avanço do Universo digital, surge a perceptível impressão de que a jurisdição não tem se integrado de forma eficaz a este novo cenário. Esse descompasso sinaliza a necessidade de adaptações normativas e procedimentais que incorporem as dinâmicas digitais, garantindo a efetividade do direito em meio às transformações tecnológicas. Segundo Lessig (1999), “o ambiente digital impõe a necessidade de repensar as leis tradicionais de forma que o Código é Lei”, sugerindo que as configurações técnicas das plataformas digitais atuam como reguladores de conduta na mesma medida que as leis escritas.

Um tema de considerável complexidade, especialmente diante das aceleradas mudanças tecnológicas, culminando notavelmente com o advento da Inteligência Artificial (IA), assunto amplamente debatido na contemporaneidade, suscita inúmeras dúvidas e evidencia diversas falhas do sistema tradicional. Diante desse cenário, este artigo, estruturado em sete tópicos, se propõe a explorar minuciosamente essas temáticas, oferecendo uma análise aprofundada e crítica sobre os impactos e desafios emergentes advindos dessas inovações tecnológicas.

No primeiro tópico, será abordado o objetivo de estabelecer os princípios e as regras vinculados às ideias de jurisdição, conforme delineados pela legislação brasileira de direito processual civil. Esta seção se dedicará a fundamentar o conceito de jurisdição, suas funções e os parâmetros legais que regem sua aplicação no contexto do sistema judiciário nacional.

O segundo tópico, serão exemplificados os desafios que o ambiente digital impõe à jurisdição tradicional. Com o crescente avanço tecnológico, surgem complexidades que questionam os limites e a eficácia das normas processuais convencionais. Esta parte da obra buscará ilustrar, por meio de exemplos práticos, como o ciberespaço desafia a aplicação das normas tradicionais de jurisdição.

No terceiro tópico, será abordado o Marco Civil da Internet no Brasil, uma legislação pioneira que visa estabelecer direitos e deveres para os usuários de plataformas digitais. Esta análise incluirá uma avaliação detalhada dos principais dispositivos da lei, suas implicações para a proteção dos direitos digitais e a sua influência na regulamentação do uso da internet no país.

O quarto e o quinto tópico, serão evidenciados os tipos de transgressões que ocorrem neste ambiente digital, bem como as dificuldades inerentes à aplicação e à fiscalização das leis

existentes. Esta seção destacará a natureza das infrações digitais, como crimes cibernéticos, e a complexidade de monitorar e aplicar sanções eficazes em um espaço tão dinâmico e amplo.

No sexto tópico, será discutida a influência das tecnologias emergentes nas normativas jurídicas. A análise se concentrará em como inovações tecnológicas, como inteligência artificial e blockchain, estão moldando novas perspectivas legais e exigindo adaptações nas legislações vigentes para assegurar uma regulação adequada e eficiente.

Finalmente, no sétimo e último capítulo, serão apresentadas propostas de reforma legal e políticas públicas voltadas para a modernização do sistema jurídico. Esta parte buscará conceituar mudanças legislativas necessárias para acompanhar a evolução tecnológica e sugerir políticas públicas que promovam a inclusão digital, a proteção dos direitos dos cidadãos no ciberespaço e a eficácia da jurisdição digital.

Destarte, esse artigo visa explorar esses tópicos propondo uma análise sobre as adequações das legislações frente aos desafios regidos pela territorialidade digital, com o objetivo de identificar soluções que possam simetrizar a necessidade de regulamentar, sem desconfigurar as liberdades fundamentais no ciberespaço.

2. JURISDIÇÃO E LIMITE TERRITORIAL

Delimitar as linhas conceituais de jurisdição e limites territoriais torna-se fator primário imprescindível. Somente após essa devida contextualização será viável avançar para a abordagem central do presente artigo. Por conseguinte, a jurisdição pode ser definida como a competência atribuída aos Órgãos do Poder Judiciário para aplicar a lei a casos concretos. De acordo com Chiovenda (1965), “a jurisdição é a função do Estado de declarar e realizar praticamente, de forma imperativa e substitutiva, a vontade da lei em relação a uma controvérsia”. Essa definição salienta dois aspectos essenciais: a autoridade do Estado e a aplicação prática da lei.

A jurisdição é verdadeiramente conceituada em diversas categorias, incluindo jurisdição contenciosa e voluntária, e pode ser subdividida em jurisdição civil, penal, trabalhista, entre outras, conforme a natureza dos conflitos. No Brasil, a Constituição Federal e o Código de Processo Civil (Lei nº 13.105/2015), delineiam os princípios e as competências jurisdicionais, assegurando que cada Ente Federativo (União, Estados, Distrito Federal e Municípios) exerçam sua jurisdição dentro dos limites territoriais assentados.

Dessa forma, a jurisdição configura-se como uma expressão da Soberania do Estado, cuja competência engloba não apenas a resolução de litígios, mas também, a proteção dos direitos e a execução das leis. Conforme exposto por Miranda (1975), “a jurisdição representa a exteriorização da Soberania do Estado, ao exercer seu poder de império sobre pessoas e bens, de forma a garantir a ordem jurídica”. Conseqüentemente, esse conceito constitui como um pilar fundamental da organização política e social de um país.

Concomitantemente, uma questão importante entra em voga: qual é a conceituação dos limites territoriais? Destarte, os limites territoriais referem-se às fronteiras físicas que demarcam a extensão da jurisdição exercida por um Estado soberano. Estes limites são estabelecidos e reconhecidos através de Legislações nacionais, decisões Judiciais e Acordos Internacionais. Sendo assim, o Direito Internacional Público desempenha um papel indispensável na definição, manutenção e resolução de disputas referentes a essas fronteiras, assegurando a soberania dos Estados e prevenindo conflitos territoriais que possam ameaçar a paz e a estabilidade global.

A difícil tarefa de estabelecer uma estabilidade jurídica consistente emerge quando há o surgimento de diversas contravenções extraterritoriais, particularmente na confluência dos limites jurisdicionais de diferentes Estados. Essas contravenções se verificam quando um ato ilícito, perpetrado fora do território de um Estado, gera efeitos ou conseqüências que afetam a ordem pública ou interesses jurídicos tutelados pelo mesmo. Considerando que os Estados dispõem de soberania restrita ao seu próprio território tal fenômeno engloba desafios significativos para a aplicação das leis e a cooperação internacional. Encontrando, assim, dificuldades substanciais para exercer jurisdição sobre atos cometidos além de suas fronteiras.

Atualmente, a natureza transnacional da internet dificulta a delimitação territorial no âmbito cibernético. A infraestrutura global da rede, caracterizada por sua interconexão e ausência de fronteiras físicas, permite que indivíduos e grupos realizem operações cibernéticas a partir de qualquer parte do mundo, desafiando profundamente as jurisdições existentes. Com este cenário, surge um ambiente desafiador de aplicação da lei e a proteção de sistemas e informações críticas, de modo que, os Estados enfrentam dificuldades significativas ao tentarem atribuir responsabilidade e penalizar os autores de tais atos, uma vez que os ataques podem atravessar múltiplas jurisdições, cada uma regida por suas próprias leis e procedimentos legais.

3. O AMBIENTE DIGITAL COMO DESAFIO À TERRITORIALIDADE TRADICIONAL

O progresso tecnológico das últimas décadas modificou significativamente o cenário social e econômico no âmbito global, resultando em um espaço digital que ultrapassa fronteiras geográficas tradicionais. Essa nova realidade acarreta grandes desafios para o conceito de territorialidade, no que tange às legislações locais e o direito Internacional. Indagações profundas sobre a aplicação e eficácia das leis embasadas em territórios físicos são levantadas por redes de comunicações que interligam indivíduos e instituições por meio do espaço cibernético. Ao contextualizar o tema, pode surgir a seguinte questão: “o que define territorialidade?”. Segundo Rodrigues (2007), “a territorialidade está fundamentada no princípio da soberania Nacional, que assegura a cada Estado o poder de legislar sobre tudo o que ocorre dentro do seu território”. Em outras palavras, significa que as pessoas, bens e atos são regidos pelas leis do país, na qual estiverem situadas, exceto em casos previstos por leis específicas.

Historicamente, a noção de territorialidade tem sido essencial para determinar a jurisdição e a competência legal (Diniz, 2024). No entanto, o conceito de ciberespaço desafia esta conjuntura, pois a internet opera em um campo que parece menosprezar as delimitações territoriais existentes. Consequentemente, surgem complexidade jurídicas quando atos praticados por jurisdição têm efeitos tangíveis em outras, estabelecendo conflitos de leis que desafiam os princípios tradicionais de soberania e controle (Lessig, 2006).

A governança da internet e a regulação das atividades digitais têm exigido uma reanálise nas estruturas legais existentes. Teóricos como Laurence Lessig e Tim Wu têm estruturado como a “arquitetura” da internet pode delimitar o comportamento humano, tanto quanto qualquer código legal. Esse parâmetro ressalta a necessidade de compreender o espaço virtual não apenas como um meio de comunicação, mas como uma plataforma própria, com regras e normas que podem divergir com as aplicadas ao espaço físicos.

Estas plataformas se consolidam progressivamente como entidades autônomas, estabelecendo suas próprias regras e normas, moldando não apenas a interação social, mas sim, a esfera econômica e política dentro do seu espaço virtual. Este fenômeno gera implicações profundas, pois confere às plataformas um papel regulador, muitas vezes comparável ao de entidades governamentais, porém sem o mesmo nível de transparência e responsabilidade.

Assim, é imperativo reconhecer este operacional não apenas como facilitador de comunicações, mas como estruturas de poder que influenciam comportamentos, mediam conflitos e, em última instância, impactam significativamente a dinâmica social.

4. O MARCO CIVIL DA INTERNET NO BRASIL

O Marco Civil da internet, instituído pela Lei nº 12.965, representa um sistema regulatório no espaço digital, estabelecendo princípios, garantias e deveres para o uso da internet no Brasil. Esta legislação, popularmente conhecida como “Constituição da Internet”, visa equilibrar a liberdade de expressão, a privacidade dos usuários e as responsabilidades dos provedores ao usarem os dados dos usuários.

A primeira proposta do Marco Civil foi concebida em 2009, com uma parceria do Ministério da Justiça e juristas da Escola de Direito do Rio de Janeiro. Essa proposta resultou em um projeto de lei registrado sob o número 2126/2011, convertido assim, na lei de número 12.956, de 23 de abril de 2014, e somente regulamentada no dia 10 de junho de 2016.

O Marco Civil é resultado de uma longuíssima discussão de aproximadamente quatro anos, entre juristas, empresas e os legisladores do país, na qual, demonstrou um sistema democrático para a concepção de tal legislação. Conforme ressalta Lemos (2014), “este processo participativo foi essencial para assegurar que as Normas refletissem as necessidades e as expectativas de diferentes segmentos da sociedade brasileira”.

A legislação cibernética foi consolidada em três princípios orientadores, (i) Fiscalizador: Institui aos Órgãos Fiscalizadores o dever de detectar as infrações cometidas no ambiente digital, tais como ANATEL e a Secretaria Nacional do Consumidor. Impõe também, o compromisso do comitê gestor da internet em promover estudos com o objetivo de regulamentar normas e padrões de neutralidade e proteção; (ii) Privacidade: Exige dos provedores de conexão e comunicação a inviabilidade dos dados dos usuários; (iii) Neutralidade: Proíbe os provedores de conexão de fazerem distinção de velocidade entre páginas da internet.

Para Lemos (2014), “o Marco Civil é, antes de tudo, um ponto de partida, e não de chegada”, ou seja, o Marco é um exemplo relevante de como a legislação pode se adaptar às novas realidades de uma sociedade conectada, porém, como qualquer lei juvenil, são

necessários certos ajustes para que suas disposições não se tornem obsoletas diante das rápidas mudanças tecnológicas.

Entretanto, para outros juristas, essa lei levanta aspectos inerentes e evidencia uma simplicidade em sua estruturação, na qual se manteve a pretensão de resolver questões de escala global, com efeitos extraterritoriais, por meio de uma legislação nacional. A própria arquitetura da internet possibilita que violações dos direitos das pessoas ocorram em qualquer parte do mundo, escapando assim da jurisdição nacional. Mesmo na tentativa de conter violações de privacidade decorrentes da coleta, armazenamento e tratamento de registros, dados pessoais ou comunicações, o artigo 11, caput, §§1º e 2º, do Marco Civil da Internet dispõe que este se aplica quando, ao menos, um dos atos ocorrer no Brasil ou quando um dos terminais estiver localizado em território nacional, obrigando pessoas jurídicas com sede no exterior a se submeterem à legislação brasileira caso possuam, ao menos, uma integrante do mesmo grupo econômico estabelecida no Brasil. Apesar da nobre intenção, a violação pode não ocorrer no Brasil, mas sim na outra extremidade da transmissão de dados, situada no exterior.

Embora a Lei nº 12.956/2014 tenha sido amplamente celebrada por ser a pioneira por disciplinar os direitos e deveres dos usuários da rede, suas lacunas normativas revelam a premente necessidade de ajustes e aprimoramentos. Estes são essenciais para garantir a efetividade das disposições legais, assegurando um equilíbrio justo e equitativo entre os interesses dos usuários e as prerrogativas dos Estados. A evolução constante das tecnologias e o dinamismo do ambiente digital demandam uma legislação que seja não apenas robusta e abrangente, mas também adaptável às novas realidades e desafios que surgem continuamente.

5. TRANSGRESSÕES NAS PLATAFORMAS DIGITAIS

A maneira que pessoas comunicam-se mudou após o surgimento das plataformas digitais, configurando uma nova forma de comunicação. Em paralelo a essa nova realidade, surgem inúmeras adversidades, especialmente no que diz respeito às transgressões digitais. Os atos inflacionários cometidos nas plataformas digitais abarcam uma ampla gama de atos ilícitos, desde crimes cibernéticos (furto de dados pessoais, ameaças, extorsões...), violação de direitos autorais e disseminação de discursos de ódio.

Um dos tópicos mais alarmantes das transgressões virtuais é a sua capacidade de ultrapassar fronteiras geográficas, colocando em ameaça o princípio da territorialidade do

direito. “A arquitetura das plataformas digitais pode tanto permitir quanto limitar certas atividades, funcionando como uma forma de regulação”. Em sua obra o autor argumenta que, na ausência de fronteiras físicas, a jurisdição tradicional torna-se complexa e, muitas vezes, ineficaz para lidar com os crimes digitais (Lessig, 1999, p. 297).

Outro aspecto importante é a disseminação de informações falsas, popularmente conhecidas como fake news, e a violação da privacidade. A propagação de fake news não só desinforma a população, mas também pode causar danos irreparáveis à reputação de indivíduos e instituições, além de influenciar negativamente decisões políticas e sociais. Shoshana Zuboff, em seu livro “The Age of Surveillance Capitalism” (2018), explora como as plataformas digitais, através da coleta massiva de dados, podem infringir a privacidade dos indivíduos e manipular comportamentos. Zuboff (2018) argumenta que essas práticas criam um novo regime econômico baseado na vigilância, onde as informações pessoais são transformadas em mercadorias para fins comerciais, sem o consentimento ou o conhecimento adequado dos usuários.

Outro ato que cresce cada vez mais são as disseminações de discursos de ódios. Segundo Letícia Cesarino, Assessora de Comunicação e Cultura do Ministério dos Direitos Humanos e da Cidadania, o discurso de ódio tende ao escalonamento e à radicalização, caso não seja combatido. Na sua avaliação, faltam meios, desenhos e metodologia para que o Estado e as políticas públicas atuem para impedir a “Soberania paralela” das plataformas digitais, a falta de transparências da política dos algoritmos das big techs, que têm permitido o patrocínio e a propagação de conteúdos criminosos.

Portanto, a responsabilidade das plataformas em relação às transgressões cometidas por seus usuários é um tema de grande debate jurídico. Julie Cohen, na sua obra “Configuring the Networked Self” (2012), aborda o papel das plataformas como intermediárias, necessitando de um equilíbrio entre a liberdade de expressão e a responsabilização por conteúdos ilícitos. Cohen (2012) enfatiza que a fiscalização deve evoluir para assegurar que as plataformas não se tornam locais de impunidades para crimes virtuais.

Diante do contexto, crimes cibernéticos representam um desafio multifacetado, o qual necessita de uma atuação Legal inovadora, sendo nítido que tamanha complexidade aflora as legislações de cada país, pois controlar algo que cresce exorbitantemente se torna um desafio.

6. DIFICULDADES DE APLICABILIDADE E FISCALIZAÇÃO

Em um cenário de crescente globalização, as plataformas digitais apresentam desafios consideráveis aos Ordenamentos Jurídicos de várias nações. Nesse contexto, o Brasil detém da Lei nº 12.965, promulgada em 23 de abril de 2014, conhecida como Marco Civil da Internet, que delinea limites e responsabilidades para os usuários no meio digital. Contudo, as efetivas aplicações e fiscalizações das disposições desta lei enfrentam obstáculos circunstanciais significativos, sendo o cerne crítico de um paradigma que transcende as barreiras físicas, no qual as jurisdições se veem confrontadas com desafios para implementar e fazer valer as normas e regulamentações existentes.

Ronaldo Lemos, em suas análises sobre direito digital, evidencia que a internet foi concebida como uma rede sem fronteira, o que dificulta as aplicações das leis. Empresas digitais como o Google, Instagram, Amazon, entre outras, operam globalmente, ficando sujeitas a uma série de legislações locais, que por sua vez, entram em contradições pelas variadas diretrizes. Para Lemos (2014), “a arquitetura aberta e transnacional da internet desafia o modelo tradicional de jurisdição baseada em fronteiras geográficas”.

Danilo Doneda argumenta que “a capacidade dos Estados de fiscalizar atividades online é limitada pela natureza descentralizada da internet e pela criptografia” (Donega, 2016). Visto que as aplicabilidades das punições são dificultadas pelas diferenças nas legislações globais sobre privacidade, proteção de dados e crimes cibernéticos. Em outros dizeres, o autor exemplifica que se uma infração for cometida em um país, e o infrator estiver localizado em outra Jurisdição, a aplicabilidade da punição se depara com uma complexidade territorial e pragmática.

As fragmentações regulatórias é outro ponto crítico evidenciado por Lemos e Donega, na qual levantam que, embora existam esforços Internacionais para criar normas comuns, como o Regulamento Geral de Proteção de Dados (GDPR), essas iniciativas ainda estão longe de ser universalmente adotadas, pois, a discrepância entre as legislações pode resultar em conflitos e duplicidade de normas, dificultando ainda mais a aplicabilidade e a fiscalização.

Para reduzir esses desafios, vários juristas e teóricos sugerem a criação de acordos Internacionais mais robustos, onde haja uma harmonização padronizada nas legislações. Porém, toda questão concerne em uma evolução no direito existente, na qual, consiga acompanhar as transformações tecnológicas. Visto que, o cenário atual traduz um sistema ainda engessado no que tange a equiparidade e aplicabilidade nas sanções jurídicas.

7. A INFLUÊNCIA DA TECNOLOGIA NAS NORMATIVAS JURÍDICAS

O direito como uma ciência antiga e clássica, estabelecido sob o manto do tradicionalismo, sempre buscou resolver os anseios da sociedade, independentemente da Era, de um modo diferente do habitual. Com a Revolução Digital, essa ciência clássica se viu compelida a enquadrar suas diretrizes a tamanha evolução tecnológica, de forma adjacente a essas transformações contínuas e significativas.

A revolução digital abalou profundamente os fundamentos do direito tradicional, exigindo uma adaptação ampla e sistemática. Essa transformação não se limitou a aspectos superficiais, mas penetrou em todos os recantos do campo jurídico, instigando uma renovação completa das práticas, procedimentos e até dos próprios conceitos legais. A tecnologia digital trouxe consigo um arsenal de ferramentas e metodologias inovadoras, que forçaram juristas, advogados, legisladores e todas as partes envolvidas no sistema jurídico a reavaliar e, muitas vezes, reimaginar a forma como o direito é praticado, interpretado e aplicado.

Nesse contexto, a evolução tecnológica impactou não apenas os processos judiciais e administrativos, mas também proporcionou uma melhoria substancial na eficiência e na eficácia do sistema jurídico como um todo. A digitalização de processos judiciais, por exemplo, facilitou o acesso à justiça, permitindo que cidadãos e profissionais do direito possam interagir com o sistema de forma mais ágil e transparente. As audiências online tornaram-se uma realidade cada vez mais comum, possibilitando a realização de sessões judiciais a distância, o que não só promove a celeridade processual, como também reduz custos e amplia o acesso à justiça, especialmente para aqueles que se encontram em localidades remotas ou com dificuldades de deslocamento.

Um avanço notável e de grande relevância foi a introdução da Inteligência Artificial (IA) nos Tribunais Jurídicos. Essa incorporação representa não apenas um marco na modernização do sistema judiciário, mas também um catalisador para a eficiência, aprimoramento da tomada de decisões e aperfeiçoamento dos processos legais. A exemplo disso, é o robô do TJRN, denominado como “Poti”, que trabalha diretamente nas execuções fiscais, realizando bloqueios e desbloqueios de valores em contas. Outra IA bem conhecida é o “Victor”, um Robô do Supremo Tribunal Federal, que analisa os Recursos Extraordinários que

sobem ao STF, com o intuito de identificar as demandas repetitivas, a fim de dar maior celeridade aos trâmites.

No entanto, esse novo cenário tem imposto grandes desafios regulatórios, especialmente no que concerne às Inteligências Artificiais (IA), que levantam questões complexas. A capacidade de sistemas IA tomarem decisões autônomas desafia os princípios tradicionais de responsabilidade e imputabilidade no direito. Neste contexto, Frank Pasquale, em sua obra “The Black Box Society” (2015), sublinha a necessidade de transparência nos algoritmos, propondo que as Normativas jurídicas segmentadas, assegurem empenho e ordenamento.

Muitos juristas temem essa evolução jurídica, pois há uma preocupação de cunho ético-moral, e o receio da superação profissional por algo maior que a mente humana. Para Zamproga (2020), “a junção e evolução só tem a contribuir com a justiça, ao oferecer dados e estatística até então desconhecidos, que poderão nortear tanto a estratégia jurídica a ser adotada pelos profissionais do direito, como a gestão de processos, seja na prestação de serviços ou na entrega da prestação jurisdicional, pelo judiciário”.

Diante do exposto, torna-se inegável que a ascensão da Revolução Digital impeliu o campo jurídico a uma metamorfose de magnitude sem precedentes. Esta mudança não apenas desafiou os paradigmas arraigados do direito tradicional, mas também estimulou uma transfiguração abrangente em suas estruturas e práticas. Contudo, este novo panorama não está isento de desafios regulatórios de monta, especialmente no que tange à integração e regulação das IA. O potencial das IA para tomarem decisões autônomas lança um desafio inédito aos princípios tradicionais de responsabilidade e imputabilidade no direito. Neste contexto, emergem preocupações ético-morais acerca do impacto dessas inovações, bem como o temor quanto à suplantação da expertise humana por entidades algorítmicas.

8. PROPOSTA DE REFORMA LEGAL E POLÍTICA PÚBLICA

A insigne frase do filósofo Heráclito (500 a.C.), “Nada é permanente, exceto a mudança”, ressoa com notável relevância nos dias atuais, manifestando de forma palpável na realidade contemporânea. Em uma sociedade imersa numa era onde a importância da existência digital rivaliza a vida analógica das pessoas, compete inegavelmente que os dispositivos tecnológicos se converteram em uma extensão intrínseca da vida das pessoas, elevando exponencialmente o valor desses ativos digitais. Frente a esse cenário, emergem conceitos como a economia digital e a cibersegurança, que ganham destaque tanto no Brasil quanto no mundo.

A economia digital constitui-se no conjunto de atividades econômicas que utilizam a internet e outras tecnologias digitais como plataforma principal, transformando substancialmente a maneira como os negócios são conduzidos e os serviços são oferecidos. Esse fenômeno é patente em diversas notícias recentes, que ilustram o crescimento exponencial das transações online, das fintechs e das plataformas de e-commerce, evidenciando a imperiosa necessidade de uma estrutura legal adaptada a essas novas dinâmicas. Por exemplo, o relatório da E-commerce Brasil assinalou um aumento significativo nas vendas online durante a pandemia, reforçando a transição para um mercado cada vez mais digital (E-commerce Brasil, 2021).

A cibersegurança, por sua vez, emerge como uma preocupação premente, na medida em que os ataques cibernéticos se tornam cada vez mais sofisticados e frequentes, demandando a implementação de medidas eficazes para proteger dados e sistemas de informação. A matéria do jornal O Globo, publicada em maio de 2023, destaca que o número de ataques cibernéticos no Brasil cresceu de forma exorbitante nos últimos três anos, pressionando empresas e governos a robustecerem suas defesas digitais (O Globo, 2023). Tais incidentes evidenciam a urgência de um arcabouço regulatório sólido, capaz de assegurar a integridade das informações e a confiança dos usuários nas plataformas digitais.

Neste contexto, a necessidade de uma reforma legal no âmbito digital se manifesta em diversas áreas do direito, incluindo a proteção de dados pessoais, a regulação das atividades comerciais eletrônicas, a governança da internet e a responsabilidade civil e penal por atos praticados online. No Brasil, a promulgação da Lei Geral de Proteção de Dados (LGPD) representa um marco significativo nesse processo de atualização normativa, estabelecendo diretrizes claras para o tratamento de informações pessoais e impondo obrigações tanto para o setor privado quanto para o setor público, com o objetivo de assegurar a privacidade e a proteção dos cidadãos em um ambiente crescentemente digitalizado. Não obstante, a LGPD constitui apenas uma peça desse complexo quebra-cabeça, sendo necessária uma abordagem holística que contemple outros aspectos igualmente relevantes.

Ademais, a questão da governança da internet, que envolve a distribuição equitativa dos recursos digitais, o acesso universal à rede e a neutralidade da rede, deve ser um ponto focal em qualquer proposta de reforma. A responsabilidade civil e penal por atos praticados online, tais como crimes cibernéticos e disseminação de fake news, deve ser rigorosamente delineada para garantir a segurança e a veracidade das informações compartilhadas no ambiente digital. A

recente discussão no Congresso Nacional acerca da atualização do Marco Civil da Internet, com propostas para incluir penalidades mais severas para a disseminação de notícias falsas, reflete a importância de uma legislação atualizada e eficaz.

9. CONCLUSÃO

A evolução das plataformas digitais tem sido uma das transformações mais significativas do nosso tempo, revolucionando tanto a maneira como vivemos quanto a forma como nos relacionamos. Desde suas origens modestas até o panorama complexo e interconectado de hoje, as plataformas digitais passaram por uma evolução revolucionária, impulsionada por avanços tecnológicos e mudanças nas necessidades e expectativas dos usuários. Essa globalização e a expansão da internet transcenderam as barreiras geográficas tradicionais, desafiando os princípios estabelecidos de jurisdição e aplicabilidade das leis, evidenciando a necessidade de uma adaptação do direito frente a essa evolução tecnológica.

O Marco Civil da Internet no Brasil, Lei nº 12.965/2014, é um exemplo significativo de esforço regulatório que busca equilibrar a liberdade de expressão, a privacidade dos usuários e as responsabilidades dos provedores de serviços online. No entanto, a efetividade dessa legislação enfrenta obstáculos consideráveis, como a ambiguidade de suas disposições, conflitos com outras legislações e dificuldades de fiscalização em um ambiente digital globalizado.

Experiências de outras localidades, tanto positivas quanto negativas, podem fornecer lições valiosas sobre como enfrentar esses desafios. Na União Europeia, por exemplo, o Regulamento Geral sobre a Proteção de Dados (GDPR) de 2018 estabeleceu um marco robusto para a proteção de dados pessoais, impondo requisitos rigorosos sobre a coleta e o processamento de dados. O GDPR é frequentemente citado como um exemplo positivo de regulamentação eficaz, que conseguiu equilibrar a proteção dos direitos dos indivíduos com a necessidade de inovação e crescimento econômico. Contudo, a implementação do GDPR também revelou desafios significativos, como a complexidade de sua aplicação e o impacto sobre pequenas e médias empresas que enfrentam dificuldades para cumprir com as exigências impostas.

Nos Estados Unidos, a abordagem regulatória tende a ser mais fragmentada e menos centralizada. Legislações como a Lei de Privacidade do Consumidor da Califórnia (CCPA) de

2018 representam esforços locais para proteger os dados dos consumidores, mas a ausência de uma legislação federal abrangente cria um mosaico regulatório que pode ser difícil de navegar tanto para os usuários quanto para as empresas. Este cenário pode levar a uma aplicação inconsistente e a lacunas na proteção dos direitos dos usuários.

Na China, a regulamentação da internet e das plataformas digitais é caracterizada por um controle governamental rigoroso. A Lei de Cibersegurança de 2017 e outras regulações subsequentes impõem fortes requisitos de censura e monitoramento. Embora essa abordagem tenha sido eficaz na manutenção do controle estatal sobre o conteúdo digital, ela também levantou preocupações significativas sobre a liberdade de expressão e os direitos humanos.

Esses exemplos demonstram que não existe uma solução única ou universal para a regulamentação das plataformas digitais. As respostas regulatórias devem ser adaptadas às particularidades culturais, econômicas e jurídicas de cada país. Ao mesmo tempo, é crucial que os sistemas jurídicos continuem a evoluir e se adaptar às mudanças tecnológicas, promovendo reformas legais que harmonizem a legislação nacional com as dinâmicas globais do ambiente digital.

Somente através de uma abordagem holística e colaborativa será possível enfrentar os desafios impostos pela digitalização e assegurar a proteção dos direitos fundamentais no ciberespaço. Isso inclui não apenas a criação de novas leis e regulamentos, mas também a cooperação internacional, o fortalecimento das capacidades de fiscalização e a promoção de uma cultura de respeito aos direitos digitais. A evolução das plataformas digitais é um fenômeno global, e a resposta a ele deve ser igualmente abrangente e inovadora para garantir um equilíbrio entre o progresso tecnológico e a proteção dos direitos fundamentais.

10. REFERÊNCIAS

BRASIL. Lei n. 10.406, 10 de janeiro de 2002. Código Civil. **Diário Oficial da União**: Seção 1, Brasília, DF. Jan. 2002. Disponível em:

<https://www.planalto.gov.br/ccivil_03/LEIS/2002/L10406compilada.htm>.

BRASIL. Lei n. 13.709, 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**: Brasília, DF. Ago. 2018. Disponível em:

<https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm>

BRASIL. Lei n. 12.965, 23 de abril de 2014. Estabelece princípios, garantas, direitos e deveres para o uso da internet no Brasil. **Diário Oficial da União**: Brasília, DF. Abr. 2014.

CHIOVENDA, Giuseppe. **Principi di Diritto Processuale Civile**. 3ª ed. Napoli: Jovene, 1995, p. 302.

COHEN, J. E. **Configuring the networked self : law, code, and the play of everyday practice**. New Haven Conn.: Yale University Press, Cop, 2012.

LEMOS, R.; FELICE, M. DI. **A Vida em rede**. [s.l.] Papyrus Editora, 2015.

LESSIG, L. **Code and other laws of cyberspace: Version 2.0**. New York: Basic Books, 2006.

SILVIO RODRIGUES. **Direito civil**. [s.l.] São Paulo Saraiva, 2007.

MARIA HELENA DINIZ. **Curso de direito civil brasileiro: Teoria geral do direito civil**. [s.l: s.n.].

MIRANDA, P. **Comentários ao Código de Processo Civil**. Rio de Janeiro: Forense, t. VII, 1975.

REIS, L. **Quase 70% das empresas no Brasil sofreram algum ataque cibernético com sequestro de dados em 2022, diz pesquisa**. Disponível em: <<https://oglobo.globo.com/economia/tecnologia/noticia/2023/05/quase70percentdasempresas-no-brasil-sofrem-ataque-cibernetico-com-sequestrodedadosem2022dizpesquisa.ghtml>>.

SMARTHINT. **E-commerce no Brasil: principais dados do mercado em 2022**. Disponível em:<<https://www.smarthint.co/ecommerce-no-brasil/#:~:text=Shopee->>. Acesso em: 19 jun. 2024.

WU, M., et al. (2010) **Research on the Architecture of Internet of Things**. 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), Chengdu, 20-22 August 2010, V5-484. - References - Scientific Research Publishing. Disponível em:

<<https://www.scirp.org/reference/referencespapers?referenceid=2792388>>. Acesso em: 19 jun. 2024.

WU, T. **The attention merchants : from the daily newspaper to social media, how our time and attention is harvested and sold.** [s.l.] London Atlantic Books, 2017.

ZUBOFF, S. **The Age of Surveillance Capitalism: The Fight for the Future at the New Frontier of Power.** London: Profile Books, 2019.

Submetido em 10.04.2024

Aceito em 06.06.2024