

REVISTA JURÍDICA DA FA7

FA7 LAW REVIEW

**Periódico Científico do Programa de Pós-Graduação em Direito
do Centro Universitário 7 de Setembro**

ISSN 1809-5836 (Impresso)

ISSN 2447-9055 (Eletrônico)

| | | | | | |
|-----------|--------|------|-----------|------|--------|
| Fortaleza | v. XXI | n. 3 | set./dez. | 2024 | 157 p. |
|-----------|--------|------|-----------|------|--------|

Catálogo na Fonte

Revista Jurídica da FA7: periódico científico do Programa de Pós-Graduação em Direito do Centro Universitário 7 de Setembro / UNI7 — v.21, n. 3 (set./dez. 2024) — Fortaleza: UNI7, 2024 [on line]

Publicação anual impressa 2004 a 2014

Publicação semestral on line a partir de 2015 disponível no portal de periódicos da UNI7 em: <https://periodicos.uni7.edu.br/index.php/revistajuridica/>

ISSN 1809-5836 (impresso)

ISSN 2447-9055 (eletrônico)

1. Periódico científico — Centro Universitário 7 de Setembro — UNI7. 2. Programa de Pós-Graduação em Direito. 3. Direito Privado. 4. Artigos Jurídicos. I. Centro Universitário 7 de Setembro — UNI7.

CDD 340.05

Revista Jurídica da FA7 / FA7 Law Review

Periódico Científico do Programa de Pós-Graduação em Direito do Centro Universitário 7 de Setembro

periodicos.uni7.edu.br/index.php/revistajuridica/ | revistajuridica@uni7.edu.br

ISSN 1809-5836 (Impresso)

ISSN 2447-9055 (Eletrônico)

Editor-Chefe

Prof. Dr. Álisson José Maia Melo

UNI7, Programa de Pós-Graduação em Direito, Fortaleza, CE, Brasil

Editor-Adjunto

Prof. Dr. Ramon de Vasconcelos Negócio

UNI7, Programa de Pós-Graduação em Direito, Fortaleza, CE, Brasil

Conselho Editorial

Prof. Dr. Antonio Fernández de Buján

Universidade Autônoma de Madri, Espanha

Prof. Dr. Carlos Eduardo Peralta Montero

Universidade da Costa Rica, Faculdade de Direito, Costa Rica

Prof.^a Dr.^a Eliane Moreira

UFPA, Faculdade de Direito, Belém, PA, Brasil

Prof. Dr. Giovanni Luchetti

Universidade de Bolonha, Departamento de Ciência Jurídica, Itália

Prof. Dr. Ignácio Maria Poveda Velasco

USP, Departamento de Direito Civil, São Paulo, SP, Brasil

Prof. Dr. João Luís Nogueira Matias

UNI7, Programa de Pós-Graduação em Direito, Fortaleza, CE, Brasil

Prof. Dr. José Isaac Pilati

UFSC, Programa de Pós-Graduação em Direito, Florianópolis, SC, Brasil

Prof.^a Dr.^a Larissa Maria de Moraes Leal

UFPE, Programa de Pós-Graduação em Direito, Recife, PE, Brasil

Prof.^a Dr.^a Laura Souza Lima e Brito
UNIBH, Curso de Graduação em Direito, Belo Horizonte, MG, Brasil

Prof.^a Dr.^a Liziane Paixão Silva Oliveira
UniCEUB, Centro Universitário de Brasília, Brasília, DF, Brasil

Prof. Dr. Luís Rodrigues Ennes
Universidade de Vigo, Espanha

Prof. Dr. Marcos Wachowicz
UFPR, Programa de Pós-Graduação em Direito, Curitiba, PR, Brasil

Prof.^a Dr.^a María José Bravo Bosch
Universidade de Vigo, Espanha

Prof.^a Dr.^a Maria Vital da Rocha
UNI7, Programa de Pós-Graduação em Direito, Fortaleza, CE, Brasil

Prof. Dr. Otavio Luiz Rodrigues Junior
USP, Universidade de São Paulo, São Paulo, SP, Brasil

Prof.^a Dr.^a Rosângela Lunardelli Cavallazzi
UFRJ, Programa de Pós-Graduação em Urbanismo; PUC/RJ, Programa de
Pós-Graduação em Direito, Rio de Janeiro, RJ, Brasil

Prof.^a Dr.^a Tarin Cristino Frota Mont'Alverne
UFC, Programa de Pós-Graduação em Direito, Fortaleza, CE, Brasil

Centro Universitário 7 de Setembro

Av. Alm. Maximiano da Fonseca, 1395 — Bairro Eng. Luciano Cavalcante
CEP: 60811-024 — Fortaleza, Ceará, Brasil
Telefone: (+55.85) 4006.7600

Programa de Pós-Graduação em Direito

Coordenador

Prof. Dr. João Luís Nogueira Matias

Área de Concentração

Relações privadas, sociedade e desenvolvimento

Linha de pesquisa 1

Relações privadas, direitos humanos e desenvolvimento

Linha de pesquisa 2

Relações privadas, mercado e desenvolvimento

Apresentação

A Revista Jurídica da FA7 / *FA7 Law Review* materializa a produção acadêmica de pesquisadores voltada à temática de “Relações Privadas e Desenvolvimento”, área de concentração do Programa de Pós-Graduação em Direito, criado no final de 2015. Destina-se à divulgação de artigos científicos, resultados de pesquisas, ensaios, traduções e resenhas, preferencialmente de autoria ou coautoria de professor-doutor.

A Revista é publicada ininterruptamente desde 2005 com periodicidade anual. Em 2015, quando foi enviada a proposta de criação do Curso de Mestrado em Direito da UNI7, o Periódico passou por uma reestruturação, a fim de se adequar aos novos rumos científicos da Instituição, passando a ter periodicidade semestral e publicação apenas eletrônica. A partir de 2020, para atender ao volume de submissões, tomou-se a decisão de reduzir a periodicidade, passando a revista a ser quadrimestral.

Posiciona-se atualmente no estrato A2, conforme avaliação do sistema WebQualis da Capes (2020).

A política editorial da Revista Jurídica da FA7 expressa a área de concentração do Programa de Pós-Graduação em Direito da UNI7, consolidada em suas linhas de pesquisa, possuindo os seguintes eixos temáticos: (i) Relações privadas, direitos humanos e desenvolvimento e (ii) Relações privadas, mercado e desenvolvimento.

Nesse sentido, este é mais um número em versão eletrônica, seguindo todas as orientações do WebQualis da Área do Direito. Essa edição é composta por 3 (três) artigos, todos submetidos à avaliação de pareceristas anônimos para a avaliação qualitativa, seguindo o sistema *double blind peer review*.

Dirige-se agradecimento aos colaboradores pelos textos aqui publicados, convidando-se os leitores a conhecerem os focos de investigação realizados, com influxo na compreensão e aplicação do Direito.

Boa leitura!

Prof. Dr. Álisson José Maia Melo

Editor-Chefe

Expediente

A Revista Jurídica da FA7 é o periódico acadêmico do Programa de Pós-Graduação em Direito do Centro Universitário 7 de Setembro (UNI7). Concentra-se na área das Relações Privadas e Desenvolvimento. Todos os números publicados em versão impressa (volumes 1 ao 11) estão também disponíveis, na íntegra, no sítio eletrônico da Revista: <https://periodicos.uni7.edu.br/index.php/revistajuridica/>.

As regras para publicação na RJFA7 encontram-se no referido sítio eletrônico da UNI7. A RJFA7 não tem fins lucrativos e é disponibilizada gratuitamente no seu portal.

O escopo e a missão do Periódico é divulgar artigos científicos de qualidade, favorecendo o diálogo científico entre pesquisadores de múltiplas instituições e países, no que diz respeito aos temas pertinentes à sua linha editorial. O volume anual é composto por duas publicações, de periodicidade semestral.

A UNI7, a Editora e o Corpo Editorial da Revista não se responsabilizam pelos dados e opiniões expressos nos artigos, sendo estes de inteira responsabilidade dos autores. Toda e qualquer correspondência, incluindo a submissão de artigos científicos, cartas aos editores, solicitação de subscrição e cópias, sugestões, avisos e outras informações, deve ser enviada ao endereço eletrônico: revistajuridica@uni7.edu.br.

É permitida a reprodução de artigos em qualquer meio, desde que citada a fonte. Considerando a política nacional de difusão do conhecimento científico, são reservados ao Centro Universitário 7 de Setembro o direito de primeira publicação. Os autores são incentivados a publicar os trabalhos em outros meios, desde que indicado o crédito da publicação original. A Revista utiliza a licença *Creative Commons vs 4.0*, com a condição “Atribuição” (CC BY 4.0).

Os autores devem estar cientes de que, se os artigos demandarem a aprovação do Comitê de Ética, deverão informar o protocolo de aprovação, anexando o respectivo Parecer. No ato da submissão, é necessário informar se há conflito de interesses com relação à pesquisa.

Sumário

Revista Jurídica da FA7

FA7 Law Review

v. XXI, n. 3, set./dez. 2024

ISSN 1809-5836 (Impresso)

ISSN 2447-9055 (Eletrônico)

AVANÇOS E DESAFIOS NA REGULAÇÃO DIGITAL COM O MARCO CIVIL DA INTERNET: PERSPECTIVAS DAS POLÍTICAS PÚBLICAS PARA A NEUTRALIDADE DA REDE

Edna Raquel Hogemann..... 13

Advances and challenges in digital regulation with the Brazilian Civil Rights Framework for the Internet: perspectives on public policies for network neutrality

MARCO CIVIL DA INTERNET E A TUTELA TRANSVERSAL DOS DIREITOS DA PERSONALIDADE: UM OLHAR SOBRE A PRIVACIDADE NA ERA DA DIGITAL E DE DESAFIOS REGULATÓRIOS INTERNACIONAIS

Daniela Menengoti Gonçalves Ribeiro 27

Adriana Rossini 27

The Brazilian Civil Rights Framework for Internet and the transversal protection of personality rights: a look at privacy in the digital and international regulatory challenges

O MARCO CIVIL DA INTERNET E A DOCTRINA DO DIÁLOGO DAS FONTES

Rogério da Silva e Souza 45

The Brazilian Civil Rights Framework for the Internet and the doctrine of the dialog of sources

MARCO CIVIL JUDICIAL DA INTERNET: PROMOVEDO DIREITOS E RESPONSABILIZAÇÃO NA NOVA ORDEM ECONÔMICA DIGITAL

André de Carvalho Ramos 61

Ricardo Luiz Nicoli 61

Brazilian Judicial Civil Rights Framework for the Internet: promoting rights and accountability in the new digital economic order

AVANÇOS E DESAFIOS NA REGULAÇÃO DIGITAL COM O MARCO CIVIL DA INTERNET: PERSPECTIVAS DAS POLÍTICAS PÚBLICAS PARA A NEUTRALIDADE DA REDE

Edna Raquel Hogemann

Universidade Federal do Estado do Rio de Janeiro (Unirio),
Rio de Janeiro.

edna.r.hogemann@unirio.br

Resumo: Este artigo explora a evolução das políticas públicas relacionadas ao Marco Civil da Internet no Brasil, analisando seus avanços, desafios e impactos na regulação digital na perspectiva da neutralidade da rede. O Marco Civil da Internet, promulgado em 2014, é uma legislação pioneira que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. A análise é dividida em três tópicos: a construção e aprovação do Marco Civil, os principais avanços e conquistas, e os desafios persistentes na sua implementação. O estudo destaca a importância de políticas públicas eficazes para assegurar uma internet livre, aberta, inclusiva e neutra o suficiente para a promoção de um ambiente digital justo e democrático.

Palavras-chave: Políticas públicas, Marco Civil da Internet, regulação digital, Brasil, neutralidade.

Advances and challenges in digital regulation with the Brazilian Civil Rights Framework for the Internet: perspectives on public policies for network neutrality

Abstract This paper explores the evolution of public policies related to the Marco Civil da Internet in Brazil, analyzing its advancements, challenges, and impacts on digital regulation from the perspective of network neutrality. Enacted in 2014, the Marco Civil da Internet is pioneering legislation that establishes principles, guarantees, rights, and duties for the use of the internet in Brazil. The analysis is divided into three topics: the development and approval of the Marco Civil, the main advancements and achievements, and the ongoing challenges in its implementation. The study highlights the importance of effective public policies to ensure a free, open, inclusive, and sufficiently neutral internet to foster a fair and democratic digital environment.

Keywords: Public policies, Marco Civil da Internet, digital regulation, Brazil, neutrality.

INTRODUÇÃO

A evolução tecnológica e a crescente digitalização da sociedade têm imposto novos desafios regulatórios, exigindo a formulação de políticas públicas eficazes que garantam um ambiente digital seguro, justo e democrático. A internet se tornou uma parte essencial da vida cotidiana, influenciando a comunicação, a economia, a educação e a política. No Brasil, o Marco Civil da Internet, sancionado em 2014, representa um marco significativo na regulação digital. É considerada uma das legislações mais importantes e inovadoras no campo da regulação digital. Ele estabelece princípios, garantias, direitos e deveres para o uso da internet no país, com especial destaque para a neutralidade da rede. A neutralidade da rede é um princípio que garante que

todos os dados na internet sejam tratados de forma igualitária, sem discriminação ou prioridade, independentemente de origem, destino, conteúdo ou tipo de serviço.

No Brasil, a implementação de políticas públicas na regulação digital é crucial para assegurar os direitos dos usuários, promover a inovação e garantir a igualdade de acesso à internet, razão pela qual o presente artigo busca analisar as políticas públicas relacionadas ao Marco Civil da Internet, avaliando seus avanços, desafios e impactos na sociedade brasileira, tendo como foco especial o dilema da neutralidade das redes. Nesse propósito o estudo inicia demonstrando em que medida o Marco civil da Internet se revela como verdadeiro exemplo de regulação digital em nosso país, trazendo uma breve reflexão a respeito de seus pilares principiológicos fundamentais. A seguir, o texto avança para se debruçar sobre os avanços e as conquistas alcançadas a partir do advento da referida lei, não sem refletir em relação aos desafios que persistem em razão de sua implementação, mormente no que diz respeito ao aspecto necessário da neutralidade da rede para, a seguir, debruçar-se sobre uma análise, ainda que não exaustiva, a respeito da importância das políticas públicas relativas à regulação digital.

O estudo conclui no sentido de apontar para a necessidade objetiva de uma internet que seja simultaneamente livre, aberta, neutra e inclusiva na perspectiva do fortalecimento das próprias políticas públicas que promovam a cooperação proativa entre governos, sociedade civil e setor privado.

1 O MARCO CIVIL DA INTERNET: UM EXEMPLO DE REGULAÇÃO DIGITAL

É evidente que o Direito se manifesta de maneira abrangente, envolvendo também a regulação do ambiente digital. Com o intuito de estabelecer diretrizes e princípios para o uso da internet no Brasil, o governo brasileiro promulgou em 2014 a Lei nº 12.965, amplamente conhecida como Marco Civil da Internet¹.

A Lei nº 12.965/14, ou Marco Civil da Internet, também denominada por alguns como a Constituição da Internet, que completou uma década desde a sua entrada em vigor em nosso ordenamento jurídico, estabelece um conjunto de princípios e diretrizes fundamentais para a regulamentação do uso da internet no Brasil. O Marco Civil da Internet é amplamente celebrado por sua natureza inovadora, tanto em termos de forma quanto de conteúdo, no que tange à regulamentação dos direitos humanos no ambiente digital. Esta legislação, composta por 32 artigos, abrange uma variedade de temas, incluindo os direitos e garantias dos usuários, a provisão de conexão e serviços da internet, a responsabilidade dos provedores e a atuação do poder público, entre outros.

Além disso, o artigo 3º dessa lei estabelece os princípios que orientam a utilização da internet no Brasil. Especificamente, ele define que a internet no Brasil deve ser guiada pelos seguintes princípios: a) Respeito à liberdade de expressão: A internet deve garantir a liberdade de expressão e acesso à informação; b) Privacidade: Deve ser assegurada a privacidade dos usuários, protegendo seus dados pessoais; c) Neutralidade da rede: As redes devem operar de forma

¹ Importante sublinhar que, “em um primeiro momento, foi submetido à sociedade um texto que continha princípios gerais para regulação da rede em que foi recebido mais de 800 comentários, opiniões e propostas que poderiam incrementar a posterior regulamentação. Em seguida, já na segunda fase do processo, as sugestões foram sistematizadas em uma minuta do projeto de lei que foi novamente submetida a consulta pública e envolveu uma série de debates públicos. Com o fim desses procedimentos, em 24 de agosto de 2011, o PL nº 2.126/2011 foi apresentado à Câmara dos Deputados, tramitando durante 3 anos entre as casas legislativas, nasceu em 2014 a Lei nº 12.965, sancionada pela presidente Dilma Rousseff na abertura da Conferência Net Mundial”. (Ramos, 2021, p. 01)

neutra, sem discriminação ou preferência por determinados conteúdos ou serviços; d) Transparência: É necessário garantir transparência nas práticas de tratamento e proteção de dados dos usuários; e) Segurança: As plataformas e serviços devem garantir a segurança dos dados. Desses, três princípios são considerados fundamentais, verdadeiros pilares da legislação: a liberdade de expressão, a neutralidade de rede e a privacidade.

O princípio da liberdade de expressão, estabelecido no inciso IX do artigo 5º da Constituição Federal, refere-se ao direito de pensar e adotar livremente ideias, bem como de participar da circulação de informações nas redes digitais sem sofrer censura. No entanto, conforme estipulado pela Constituição, o anonimato é vedado, o que implica que esse direito não é absoluto e que o indivíduo pode ser responsabilizado civil ou criminalmente caso exceda os limites estabelecidos para a expressão.

O segundo pilar é a neutralidade de rede, prevista no artigo 9º do Marco Civil da Internet, será detalhadamente analisada em tópico próprio no presente estudo, na medida em que compõe objeto de reflexão deste. No entanto, é possível, desde já, afirmar que este princípio determina que os provedores de internet devem tratar todos os pacotes de dados de maneira equânime, sem discriminação com base no conteúdo, origem, destino ou aplicação dos dados. A neutralidade de rede, um dos aspectos mais controversos durante a discussão do projeto de lei, assegura que os usuários possam acessar qualquer conteúdo na internet sem que os provedores possam interferir na velocidade da navegação ou bloquear o acesso a determinados sites.

Por fim, a privacidade, também garantida pelo artigo 5º da Constituição Federal, é um dos pilares fundamentais do Marco Civil da Internet. Este princípio visa proteger os dados pessoais dos usuários, exigindo seu consentimento expresso para qualquer operação realizada com essas informações. Além disso, a lei prevê a possibilidade de indenização por danos materiais ou morais resultantes de violações à intimidade, comunicações sigilosas e à vida privada dos usuários.

No que se refere aos direitos e garantias dos usuários da internet, o artigo 7º da Lei nº 12.965/14 é enfático ao assegurar a inviolabilidade e o sigilo tanto do fluxo das comunicações quanto das comunicações privadas armazenadas, salvo em casos específicos autorizados por ordem judicial. Este dispositivo legal proporciona uma proteção robusta contra a exposição não autorizada das informações pessoais dos usuários, garantindo que estas só possam ser acessadas em situações excepcionais e devidamente justificadas.

O artigo 10º, § 1º da mesma lei detalha de maneira específica as normas para a proteção dos registros, dados pessoais e comunicações privadas. Ele esclarece que, no caso de requisição judicial, o responsável pela guarda desses dados está legalmente obrigado a disponibilizá-los. Essa obrigação decorre da necessidade de cumprimento de ordens judiciais e é essencial para garantir a eficácia de investigações e procedimentos legais que requerem o acesso a informações privadas.

Ademais, a lei estipula que a recusa em fornecer os dados solicitados por uma ordem judicial pode ter consequências legais severas. Especificamente, se o responsável pela guarda dos dados se negar a atender a uma requisição judicial, ele poderá ser considerado culpado pelo crime de desobediência, conforme previsto no artigo 330 do Código Penal Brasileiro. Tal disposição reforça a importância do cumprimento das ordens judiciais e a seriedade das implicações jurídicas para a não colaboração com o processo judicial.

Esses dispositivos refletem o equilíbrio que o Marco Civil da Internet busca estabelecer entre a proteção dos direitos individuais dos usuários e a necessidade de acesso a informações para fins legais e de segurança pública.

A aplicação rigorosa dessas normas é crucial para assegurar que a privacidade e a segurança dos dados dos usuários sejam mantidas, ao mesmo tempo que as autoridades têm as ferramentas necessárias para realizar investigações e manter a ordem. Segundo Polido e Doneda (2015), "o processo de construção do Marco Civil foi um exemplo notável de participação cidadã e transparência na formulação de políticas públicas no Brasil". A proposta inicial foi apresentada em 2009, e após um extenso debate público, o projeto foi aprovado pelo Congresso Nacional e sancionado pela Presidência da República em abril de 2014.

Como demarcado, o Marco Civil estabelece esses princípios fundamentais como a neutralidade da rede, a privacidade e a proteção de dados pessoais, a liberdade de expressão e a garantia de direitos humanos no ambiente digital. De acordo com Doneda (2014), "o Marco Civil da Internet é uma das legislações mais avançadas do mundo no que diz respeito à regulação da internet, estabelecendo um equilíbrio entre direitos individuais e interesses coletivos". A neutralidade da rede impede práticas discriminatórias, promovendo um ambiente digital competitivo e inovador.

2 AVANÇOS E CONQUISTAS DO MARCO CIVIL DA INTERNET

Apesar de sua publicação em 23 de junho de 2014, o Marco Civil da Internet enfrentou questionamentos quanto a diversos de seus artigos, uma vez que muitas das questões abordadas na lei requeriam regulamentação adicional. Em resposta a essas necessidades, o governo federal editou o Decreto nº 8.771, em 2016, para esclarecer e regulamentar aspectos específicos, como a discriminação de pacotes de dados e a degradação do tráfego, os procedimentos para a guarda e proteção de dados por provedores de conexão e de aplicações, as medidas de transparência nas requisições de dados pela administração pública e os parâmetros para fiscalização e apuração de infrações.

Em relação ao legado do Marco Civil da Internet, é importante destacar que, com sua implementação, o Brasil estabeleceu-se como uma referência global na formulação de princípios fundamentais para uma internet livre e aberta, que garante os direitos dos usuários. O marco legal recebeu elogios de destacadas figuras do contexto digital, incluindo Tim Berners-Lee, criador da World Wide Web (WWW). Além disso, a legislação brasileira inspirou a Declaração Italiana de Direitos da Internet, influenciou as reformas legislativas na França voltadas à inclusão de direitos digitais e foi mencionada pela Suprema Corte da Argentina em uma decisão sobre a responsabilidade dos provedores de busca em relação aos resultados indexados (Ramos, 2021).

Desde sua promulgação e ao longo desses dez anos de vigência, o Marco Civil da Internet trouxe diversos avanços significativos para a regulação digital no Brasil. Um dos principais avanços é a garantia da neutralidade da rede, que impede provedores de internet de discriminar ou priorizar determinados tipos de conteúdo, aplicativos ou serviços. Esta medida assegura um ambiente digital justo e competitivo, promovendo a inovação e a liberdade de escolha dos usuários. a garantia da neutralidade da rede tem sido fundamental para manter a internet como um espaço livre e democrático. Este princípio impede que provedores de serviços de internet (ISPs) favoreçam ou bloqueiem determinados conteúdos, garantindo que todos os usuários tenham igual acesso à informação e aos serviços online. Isso promove um ambiente de inovação, onde novas empresas e ideias podem competir em pé de igualdade com os gigantes estabelecidos.

Outro avanço importante é a proteção da privacidade e dos dados pessoais dos usuários. O Marco Civil estabelece que os dados dos usuários só podem ser coletados, armazenados e utilizados com o consentimento expresso dos mesmos, e que os provedores de internet são responsáveis pela segurança dessas informações. Conforme afirma Bioni (2016), "a proteção de

dados pessoais no Marco Civil da Internet representa um passo crucial para a consolidação de um ambiente digital seguro e confiável". De tal modo que a legislação brasileira é vista como um exemplo global de como equilibrar a proteção dos direitos individuais com a necessidade de segurança e transparência no uso dos dados.

Além disso, o Marco Civil reforça a liberdade de expressão, garantindo que os usuários possam se expressar livremente na internet, sem medo de censura ou retaliação. Esta garantia é essencial para a promoção de uma sociedade democrática e pluralista, onde diversas vozes e opiniões podem ser ouvidas.

3 DESAFIOS PERSISTENTES NA IMPLEMENTAÇÃO DO MARCO CIVIL DA INTERNET E NA IMPLEMENTAÇÃO DA NEUTRALIDADE DA REDE

O fato de o Marco Civil da Internet estar em vigor em nosso país desde 2014 não impediu que em 2021, o Tribunal de Justiça do Estado do Rio Grande do Sul (TJRS) tenha sido alvo de um ataque cibernético significativo, que expôs as vulnerabilidades de sistemas críticos e destacou a importância da proteção de dados pessoais e da segurança online. Este incidente foi um dos mais notáveis no Brasil, refletindo a crescente sofisticação e frequência dos ataques cibernéticos contra instituições públicas e privadas.

O ataque ao TJRS ocorreu em maio de 2021 e foi caracterizado por um *ransomware*, um tipo de malware que criptografa os dados da vítima e exige um resgate para a sua liberação. Os invasores conseguiram acessar e comprometer os sistemas internos do tribunal, afetando severamente a operação de diversos serviços e sistemas judiciais. O *ransomware* utilizado foi uma variação do grupo de malware conhecido como "Conti," que é famoso por suas operações agressivas e pela demanda de resgates elevados.

Em Maio de 2021 o TJRS sofreu um ataque hacker que paralisou as atividades de forma total, num prejuízo mais grave do que a própria pandemia e o trabalho remoto frente a pandemia trouxe, com efeitos que mais de 3 meses depois continuam reverberando para todas as partes envolvidas, seja advocacia, serventuários, cidadãos.

Em Julho de 2021 a polícia apreendeu computadores na casa de um servidor do Tribunal ligado ao setor de informática e afirmam terem localizado indícios de que na casa de uma juíza haveria também a possibilidade de que as invasões ao TJRS tivessem sido originárias destes locais. (Rocha, 2021, p. 01)

O impacto do ataque foi extenso e multifacetado: O TJRS enfrentou uma paralisação significativa de seus serviços digitais, incluindo o sistema de processos judiciais, consultas públicas e outras funções essenciais. Isso gerou atrasos em processos legais e causou transtornos para advogados, partes envolvidas e o público em geral. Embora não tenha sido confirmado que dados sensíveis foram diretamente acessados ou divulgados, a criptografia de arquivos e o bloqueio de sistemas levantaram preocupações sobre a possível exposição de informações pessoais e confidenciais de cidadãos e funcionários.

A recuperação do ataque demandou consideráveis recursos financeiros e humanos. O TJRS precisou investir em serviços de cibersegurança para restaurar seus sistemas e garantir a integridade dos dados, além de revisar e fortalecer suas medidas de segurança. O ataque também afetou a reputação do tribunal, minando a confiança pública na capacidade da instituição de proteger informações sensíveis e garantir a continuidade dos serviços.

Cumpra ressaltar que o incidente com o TJRS sublinha várias questões críticas sobre a proteção de dados pessoais e a segurança online: A ocorrência destaca a importância de investir em medidas de segurança cibernética robustas e atualizadas, incluindo sistemas de defesa contra *ransomware*, criptografia de dados e práticas de segurança contínuas. Também mostrou ser essencial promover a conscientização sobre cibersegurança entre funcionários e usuários. Treinamentos regulares sobre *phishing* e outras ameaças podem ajudar a prevenir ataques. Razão pela qual as instituições precisam desenvolver planos de resposta a incidentes eficazes para minimizar o impacto de ataques e garantir a rápida recuperação dos serviços.

Esse ataque reforça a necessidade de conformidade com leis e regulamentações de proteção de dados, como a Lei Geral de Proteção de Dados (LGPD) no Brasil, que impõe responsabilidades sobre o tratamento e segurança das informações pessoais. E, por outro lado, aponta para a necessidade da colaboração entre organizações e o compartilhamento de informações sobre ameaças que podem melhorar a detecção e a resposta a incidentes cibernéticos.

O ataque ao Tribunal de Justiça do Rio Grande do Sul em 2021 serve como um lembrete contundente da crescente ameaça cibernética enfrentada por instituições públicas e privadas. A proteção de dados pessoais e a segurança online devem ser priorizadas para assegurar a integridade das informações e a continuidade dos serviços essenciais. A experiência adquirida com o incidente oferece lições valiosas para fortalecer a resiliência e a segurança em um ambiente digital cada vez mais complexo e desafiador.

Após 10 anos de sua vigência, a lei tem enfrentado diversos desafios em sua aplicação, gerando debates sobre a necessidade de uma atualização. Um exemplo disso pode-se perceber no que diz respeito ao fato de apesar da evidente clareza do dispositivo do art. 3º, anteriormente referido no presente estudo, persiste a argumentação de que as plataformas digitais apenas seriam responsáveis conforme o disposto no art. 19, que aborda a responsabilidade em relação ao conteúdo publicado pelos usuários. Em outras palavras, observa-se uma negligência na interpretação sistemática das leis, resultando na omissão da aplicação da responsabilidade das plataformas em relação às suas atividades de moderação de conteúdos, como impulsionamento, recomendação, e restrição de alcance de conteúdos e contas. Essa postura tem sido benéfica para essas empresas, mas extremamente prejudicial para a sociedade brasileira em larga escala.

3.1 A questão da neutralidade na rede

Barbosa recorda que a neutralidade de rede foi um dos temas divergentes que dificultou a aprovação da matéria. "Na época, [a neutralidade] foi o tema que gerou maior discordância entre empresas e sociedade civil e pesquisadores naquele momento, porque o Brasil vinha avançando para um modelo de comercialização de serviços de acesso à Internet que poderia chegar num estágio em que você teria pacotes mais baratos, em que o usuário só acessaria, por exemplo, e-mail e redes sociais. Outros pacotes mais caros em que você poderia assistir vídeos", disse a jornalista, que atualmente integra a organização Direito à Comunicação e Democracia (Dira-Com) e é uma das representantes da sociedade civil no Comitê Gestor da Internet no Brasil (CGL.br). (Urupá. 2024, p. 01)

Aqui exsurge com destaque o que prevê o art. 9º do Marco Civil, qual seja o denominado princípio da neutralidade da rede, o qual assegura que os provedores de internet tratem todos os pacotes de dados de forma igualitária, sem distinção por conteúdo, origem, destino, serviço, terminal ou aplicação. O caput do artigo referido assim dispõe: "Art. 9º O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação." Ou seja,

o artigo estabelece que todos os pacotes de dados que transitam pela rede devem receber tratamento isonômico. Isso significa, tecnicamente, que os bits que trafegam pela rede mundial não devem ser discriminados com base em sua origem, destino, conteúdo, terminal ou aplicação, tornando vedadas tais práticas discriminatórias.

Além disso, revela-se pertinente trazer à lume o que está disposto no conteúdo dos incisos I, II, III e IV do parágrafo 2º e 3º do art. 9º, que estabelecem disposições referentes à responsabilidade por práticas de discriminação ou degradação no tráfego da web, a saber:

§ 2º Na hipótese de discriminação ou degradação do tráfego prevista no § 1º, o responsável mencionado no caput deve:

I – abster-se de causar dano aos usuários, na forma do art. 927[1] da Lei no 10.406, de 10 de janeiro de 2002 – Código Civil;

II – agir com proporcionalidade, transparência e isonomia;

III – informar previamente de modo transparente, claro e suficientemente descritivo aos seus usuários sobre as práticas de gerenciamento e mitigação de tráfego adotadas, inclusive as relacionadas à segurança da rede; e

IV – oferecer serviços em condições comerciais não discriminatórias e abster-se de praticar condutas anticoncorrenciais.

3º Na provisão de conexão à internet, onerosa ou gratuita, bem como na transmissão, comutação ou roteamento, é vedado bloquear, monitorar, filtrar ou analisar o conteúdo dos pacotes de dados, respeitado o disposto neste artigo.

Em conformidade com o disposto no inciso I do § 2º do art. 9º, que remete ao artigo 927 do Código Civil – Lei 10.406/02, a responsabilidade pela reparação de danos decorrentes de atos ilícitos (arts. 186 e 187) é atribuída àqueles que os causarem. Assim, os dispositivos legais mencionados impedem que os provedores de conexão restrinjam o acesso dos usuários a determinados serviços e garantem que todos os provedores e operadoras de serviços de internet ofereçam pacotes que não discriminem os usuários, especialmente no que se refere ao acesso a sites específicos.

Em termos mais claros, as entidades responsáveis pela prestação de serviços de rede estão proibidas de discriminar os serviços oferecidos aos usuários ou de estabelecer restrições diferenciadas no acesso individual dos usuários. Ou seja, todos os usuários devem gozar de direitos iguais. Assim é possível referir-se à neutralidade da rede como proibição de modificações na velocidade e na qualidade do serviço pelos provedores em relação a conteúdos, destinos de acesso ou ao uso de produtos de concorrentes. Um exemplo disso é a prática de reduzir a velocidade de conexão para programas de Voz sobre IP (VOIP), como o SKYPE. A neutralidade da rede tornou-se uma norma, e qualquer provedor que a viole deverá justificar suas ações.

A neutralidade da rede foi um tema amplamente debatido durante a discussão e aprovação da Lei nº 12.965/14, pois a sua implementação contrariou interesses de grandes organizações nacionais fornecedoras de serviços de Internet. A referida lei legalizou e, consequentemente, burocratizou a prestação desses serviços, mas ao mesmo tempo, assegurou direitos e proteção aos usuários da rede.

Atualmente, considerando a importância da internet na vida cotidiana, a ausência de um Marco Civil da Internet, que estabelecesse os princípios jurídicos fundamentais para o uso da rede, resultaria na falta do princípio da neutralidade da rede e, certamente, tal ausência poderia ter consequências negativas significativas, expondo os usuários a diversos riscos associados à internet. Entre os quais podem ser citados, a título exemplar, ainda que sem a pretensão de esgotar a temática:

- a) Discriminação de Conteúdos: Provedores de serviços poderiam priorizar ou penalizar determinados conteúdos com base em acordos comerciais ou interesses próprios, prejudicando a liberdade de acesso e a diversidade de informações.
- b) Distorção da Competição: Empresas de maior porte poderiam pagar para garantir maior velocidade e visibilidade para seus serviços, desfavorecendo startups e concorrentes menores que não possuem recursos financeiros para competir em termos de velocidade e acesso.
- c) Restrição ao Acesso a Serviços: Usuários poderiam enfrentar limitações no acesso a serviços específicos, como plataformas de comunicação e ferramentas de colaboração, caso tais serviços sejam favorecidos ou prejudicados pelos provedores.
- d) Aumento dos Custos para Usuários: A introdução de diferentes pacotes e tarifas para acessar diferentes tipos de conteúdo e serviços poderia elevar os custos para os usuários, afetando negativamente o acesso à informação e a inclusão digital.
- e) Impacto na Liberdade de Expressão: A possibilidade de provedores limitarem ou priorizarem certos conteúdos pode afetar a liberdade de expressão, limitando a capacidade dos indivíduos de compartilhar e acessar informações de forma equitativa.
- f) Redução da Inovação: A falta de neutralidade pode desencorajar a inovação tecnológica, pois novos serviços e aplicativos podem enfrentar barreiras artificiais impostas por provedores que favorecem concorrentes estabelecidos.
- g) Prejuízo à Privacidade: Provedores poderiam monitorar e manipular o tráfego de dados de acordo com interesses comerciais, comprometendo a privacidade dos usuários e a segurança das informações pessoais.

De todo modo, e apesar dos avanços significativos, é importante demarcar que a implementação da neutralidade da rede no Brasil enfrenta diversos desafios. Um dos principais é a fiscalização eficaz deste princípio. A Agência Nacional de Telecomunicações (Anatel) é a responsável por regulamentar e fiscalizar os ISPs, mas enfrenta dificuldades técnicas e orçamentárias para realizar essa tarefa de forma plena. A complexidade técnica da gestão de tráfego de dados e a falta de recursos adequados dificultam a identificação e punição de práticas que violam a neutralidade da rede.

Um dos principais desafios é a aplicação efetiva da neutralidade da rede. Segundo Rodrigues (2018, p. 60), "a fiscalização e a garantia da neutralidade da rede são tarefas complexas, que exigem uma coordenação eficaz entre diferentes órgãos reguladores e a participação ativa da sociedade civil".

Outro desafio significativo é a proteção da privacidade e dos dados pessoais. Embora o Marco Civil estabeleça diretrizes claras, a implementação prática dessas medidas enfrenta obstáculos, como a falta de recursos e a necessidade de aprimoramento das capacidades técnicas dos órgãos responsáveis pela fiscalização. Além disso, a crescente incidência de crimes cibernéticos e vazamentos de dados exige uma atualização constante das políticas de segurança e proteção de dados.

Há que ser apontado um importante desafio a ser enfrentado consubstanciado pela pressão das grandes empresas de telecomunicações. Esses conglomerados possuem recursos significativos e frequentemente exercem influência política para tentar flexibilizar as regras de neutralidade, alegando que a capacidade de gerenciar o tráfego de dados é essencial para a manutenção de um serviço de alta qualidade. Segundo estudos, em diversos momentos houve tentativas de

lobby para alterar a legislação em favor desses interesses, o que poderia comprometer a igualdade de acesso à internet.

Por fim, a garantia da liberdade de expressão na internet também enfrenta desafios. A disseminação de desinformação e discurso de ódio nas plataformas digitais representa uma ameaça à integridade do ambiente digital. Conforme observa Gagliardi (2020), "é necessário encontrar um equilíbrio entre a proteção da liberdade de expressão e a prevenção de abusos que possam comprometer a harmonia social e a democracia".

Para enfrentar esses desafios, é crucial que o Brasil desenvolva políticas públicas robustas e eficazes. A participação ativa da sociedade civil e de organizações não governamentais é fundamental para garantir que a implementação do Marco Civil continue a proteger os direitos dos usuários. Campanhas de conscientização e educação digital podem ajudar os cidadãos a entenderem seus direitos e a identificarem violações, pressionando por uma internet mais justa e equitativa.

4 A IMPORTÂNCIA DAS POLÍTICAS PÚBLICAS NA REGULAÇÃO DIGITAL

É essencial que o governo e as agências reguladoras invistam em capacidades técnicas e recursos para a fiscalização. A cooperação internacional também pode ser uma ferramenta valiosa, permitindo a troca de experiências e melhores práticas com outros países que enfrentam desafios semelhantes na regulação da neutralidade da rede.

Além do Marco Civil da Internet, diversas outras políticas públicas têm sido desenvolvidas para aprimorar a regulação digital no Brasil. Entre essas iniciativas, destaca-se a Lei Geral de Proteção de Dados (LGPD), que foi sancionada em 2018 e representa um marco significativo na legislação brasileira sobre a proteção de dados pessoais. A LGPD, inspirada no Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, tem como objetivo central estabelecer normas rigorosas para o tratamento e a proteção de dados pessoais, refletindo uma preocupação crescente com a privacidade dos indivíduos na era digital.

A LGPD cria um conjunto de diretrizes e princípios que regulamentam a coleta, o armazenamento, o processamento e a utilização de dados pessoais. Essas diretrizes visam assegurar que os dados dos cidadãos sejam tratados de forma ética e transparente, garantindo que os indivíduos tenham controle sobre suas próprias informações. A lei exige que as organizações obtenham o consentimento explícito dos titulares de dados antes de processar suas informações, e estabelece a obrigatoriedade de informar claramente sobre a finalidade do uso desses dados.

Além disso, a LGPD institui direitos específicos para os titulares de dados, como o direito à confirmação da existência de tratamento, o direito de acesso às informações, e o direito de correção de dados incompletos, inexatos ou desatualizados. A lei também prevê mecanismos para que os indivíduos possam revogar seu consentimento a qualquer momento e solicitar a exclusão de seus dados pessoais.

Outro aspecto importante da LGPD é a criação da Autoridade Nacional de Proteção de Dados (ANPD), responsável por fiscalizar e assegurar o cumprimento da legislação. A ANPD tem a competência para aplicar sanções e multas às organizações que não aderirem às normas estabelecidas, além de promover orientações e esclarecimentos sobre a aplicação da lei.

Portanto, a LGPD representa um avanço significativo na proteção dos dados pessoais no Brasil, alinhando-se às melhores práticas internacionais e reforçando o compromisso com a privacidade e a segurança das informações dos cidadãos. Essa legislação complementa e fortalece o Marco Civil da Internet, oferecendo um framework mais robusto para enfrentar os desafios da era digital e garantir a proteção dos direitos dos usuários.

A LGPD impõe obrigações rigorosas às empresas e organizações que coletam e processam dados pessoais, exigindo medidas de segurança adequadas e a obtenção de consentimento claro dos usuários. Bioni (2016) destaca que "a proteção de dados pessoais no Brasil representa um passo crucial para a consolidação de um ambiente digital seguro e confiável" (p. 50).

Para enfrentar os desafios complexos da regulação digital, é essencial que as políticas públicas sejam elaboradas de forma participativa e transparente. Este processo deve envolver ativamente diversos stakeholders, incluindo a sociedade civil, organizações não governamentais (ONGs) e o setor privado, para assegurar que as políticas reflitam as necessidades e preocupações de todos os envolvidos.

A participação ativa da sociedade civil é crucial para a criação de políticas que realmente atendam às demandas da população. Por exemplo, a implementação da Lei Geral de Proteção de Dados (LGPD) no Brasil resultou de um processo de consulta pública extensivo, no qual foram coletadas contribuições de cidadãos, especialistas e empresas. Essa abordagem ajudou a moldar uma legislação que equilibrasse a proteção da privacidade com a necessidade de inovação e crescimento econômico. A participação de ONGs, como a Data Privacy Brasil, foi fundamental para garantir que a lei atendesse às preocupações sobre a coleta e o uso de dados pessoais.

Além do mais, o envolvimento do setor privado também é importante para garantir a viabilidade e a aplicabilidade das políticas. Empresas de tecnologia, por exemplo, podem fornecer insights valiosos sobre a implementação prática de regulamentações e colaborar na criação de soluções técnicas que atendam aos requisitos legais. Um exemplo disso é o trabalho conjunto entre plataformas de redes sociais e reguladores para implementar medidas de combate à desinformação e proteger a integridade das eleições. Plataformas como o Facebook e o Twitter têm colaborado com entidades reguladoras para desenvolver e aprimorar políticas que abordem a disseminação de informações falsas e o impacto na opinião pública.

Campanhas de conscientização e educação digital são ferramentas eficazes para empoderar os cidadãos e promover uma internet mais justa e equitativa. Essas campanhas ajudam os usuários a entenderem seus direitos e a reconhecerem possíveis violações, além de fornecerem informações sobre como agir em casos de abuso. Por exemplo, iniciativas como o "Safer Internet Day" promovem a educação sobre segurança online e proteção de dados pessoais, incentivando o engajamento dos usuários em práticas seguras e responsáveis na internet.

Essas ações coletivas são essenciais para a construção de um ambiente digital que respeite os direitos dos indivíduos e promova a justiça social. A formulação de políticas públicas eficazes depende de uma colaboração contínua e transparente entre todos os stakeholders, garantindo que as regulamentações sejam justas, aplicáveis e adaptadas às necessidades reais da sociedade.

A cooperação internacional é essencial para aprimorar as políticas de regulação digital, e a troca de experiências e melhores práticas entre países desempenha um papel fundamental nesse processo. Ao colaborar com organismos internacionais e adotar padrões globais, o Brasil pode fortalecer a proteção dos direitos dos usuários e criar um ambiente digital mais seguro e eficiente.

Um exemplo notável dessa cooperação é a participação do Brasil no Grupo de Trabalho sobre Governança da Internet da OCDE. Através desse grupo, o Brasil tem acesso a diretrizes e práticas recomendadas por países que lideram a regulação digital, como os membros da União

Europeia e os Estados Unidos. A troca de experiências com essas nações permite que o Brasil adote abordagens comprovadas para questões como a proteção de dados pessoais e a segurança cibernética. Por exemplo, a experiência da União Europeia com o Regulamento Geral sobre a Proteção de Dados (GDPR) tem sido uma referência crucial para a Lei Geral de Proteção de Dados (LGPD) do Brasil, que incorporou muitos dos princípios e práticas do GDPR para assegurar um padrão elevado de proteção de dados.

Outro exemplo é a colaboração do Brasil com a Comissão Internacional de Proteção de Dados (ICDP) e a Rede Internacional de Autoridades de Proteção de Dados e Privacidade (IDP). Essas organizações oferecem um fórum para discutir desafios globais e compartilhar soluções em matéria de proteção de dados. Através dessa rede, o Brasil tem participado de debates sobre a implementação de mecanismos de conformidade e fiscalização, beneficiando-se das experiências de outros países que já enfrentaram desafios semelhantes (ANPD, 2022).

Além disso, a cooperação internacional também é evidenciada pelo envolvimento do Brasil em iniciativas globais contra a desinformação e o discurso de ódio online. A participação em fóruns internacionais, como o Fórum Global sobre Segurança Cibernética e o Fórum de Governança da Internet da ONU, permite ao Brasil colaborar com outras nações para desenvolver estratégias eficazes de combate a ameaças digitais. Por exemplo, a colaboração com países da União Europeia na criação de diretrizes para o combate à desinformação ajudou o Brasil a desenvolver políticas mais robustas e alinhadas com padrões globais.

Essas experiências demonstram que a cooperação internacional não apenas facilita o acesso a melhores práticas e soluções inovadoras, mas também contribui para a criação de um ambiente digital mais seguro e justo. Através do intercâmbio de conhecimentos e da adoção de padrões globais, o Brasil pode aprimorar suas políticas de regulação digital e proteger efetivamente os direitos dos usuários.

CONCLUSÃO

Caminha-se para a conclusão do presente ensaio no qual buscou-se demonstrar em que medida o Marco Civil da Internet no Brasil representa um marco significativo na regulação digital, especialmente no que se refere à neutralidade da rede. Ao longo do texto foi possível perceber que essa normativa, sancionada em 2014, estabelece princípios fundamentais para a utilização da internet, como a liberdade de expressão, a privacidade dos usuários e a neutralidade da rede, que garante que todos os dados trafeguem pela mesma rede sem discriminação. No entanto, a implementação e a efetividade desses princípios enfrentam desafios consideráveis que exigem uma atuação contínua e integrada de diversos setores da sociedade.

O avanço promovido pelo Marco Civil da Internet é evidente, mas não é isento de dificuldades. A sua implementação bem-sucedida depende da coordenação entre políticas públicas eficazes, uma fiscalização rigorosa e a participação ativa dos cidadãos. Sem esses elementos, a promessa de uma internet livre, aberta e inclusiva pode ser comprometida. Para garantir que a internet continue a ser um espaço de igualdade de acesso e inovação, é crucial que o Brasil mantenha um compromisso sólido com a regulação digital.

A importância das políticas públicas na regulação digital é inegável. O Marco Civil da Internet e a Lei Geral de Proteção de Dados (LGPD), sancionada em 2018, representam avanços significativos na proteção dos direitos dos usuários e na promoção de um ambiente digital justo e democrático. A LGPD, inspirada pelo Regulamento Geral sobre a Proteção de Dados (GDPR)

da União Europeia, estabelece diretrizes rigorosas para o tratamento e proteção de dados pessoais. Essas leis são essenciais para proteger a privacidade dos usuários e garantir que suas informações sejam utilizadas de forma transparente e ética.

Por outro lado, a implementação dessas políticas enfrenta vários desafios. Por exemplo, o Marco Civil da Internet enfrenta dificuldades na aplicação efetiva de princípios como a neutralidade da rede e a proteção de dados pessoais, especialmente com a rápida evolução da tecnologia e a crescente complexidade das plataformas digitais. A fiscalização das práticas de coleta e uso de dados, bem como a proteção contra abusos e a promoção da transparência, requerem esforços contínuos e atualizações regulares das diretrizes.

A participação social desempenha um papel crucial na regulação digital. A colaboração ativa de cidadãos, organizações não governamentais e do setor privado é essencial para garantir que as políticas atendam às necessidades e preocupações de todos os stakeholders. Campanhas de conscientização e educação digital ajudam a empoderar os cidadãos, permitindo-lhes compreender seus direitos e identificar possíveis violações. Por exemplo, a iniciativa "*Safer Internet Day*" promove a educação sobre segurança online e proteção de dados pessoais, incentivando práticas responsáveis e seguras entre os usuários da internet.

Além da participação nacional, a cooperação internacional é vital para aprimorar as políticas de regulação digital. A troca de experiências e melhores práticas com outros países pode fornecer insights valiosos e ajudar o Brasil a adotar abordagens mais eficazes. A participação em fóruns internacionais, como o Fórum Global sobre Segurança Cibernética e o Fórum de Governança da Internet da ONU, permite ao Brasil colaborar com outras nações para desenvolver estratégias globais de proteção de dados e combate à desinformação. A experiência internacional, como a implementação do GDPR na União Europeia, oferece lições importantes que podem ser adaptadas às necessidades brasileiras.

A atualização constante das diretrizes e a melhoria das capacidades técnicas e de fiscalização são fundamentais para enfrentar os desafios emergentes. As rápidas inovações tecnológicas e o surgimento de novas ameaças digitais exigem que as políticas de regulação digital sejam adaptáveis e responsivas. O aprimoramento contínuo das práticas de fiscalização, bem como a integração de novas tecnologias e metodologias, é essencial para garantir que a proteção dos direitos digitais seja eficaz e abrangente.

Finalmente, para assegurar uma internet que seja livre, aberta e inclusiva, é essencial fortalecer as políticas públicas e promover a cooperação entre governo, sociedade civil e setor privado. A integração dessas partes interessadas, aliada à atualização constante das diretrizes e à melhoria das capacidades de fiscalização, permitirá ao Brasil enfrentar os desafios emergentes e garantir a proteção dos direitos digitais de forma justa e eficaz. Com esses esforços coordenados, o Brasil pode continuar a servir como um exemplo global de regulação digital justa e democrática.

REFERÊNCIAS

ANPD. **Participação da ANPD no cenário internacional e a regulamentação de transferências internacionais de dados pessoais**. 2022. Disponível em: <https://www.gov.br/anpd/pt-br/asuntos/semana-da-protexcao-de-dados-2022/participacao-da-anpd-no-cenario-internacional-e-a-regulamentacao-de-transferencias-internacionais-de-dados-pessoais>. Acesso em 30 jun. 2024.

BIONI, B. Proteção de Dados Pessoais: A Função e os Limites do Consentimento. In: **Revista Brasileira de Direito das Telecomunicações**, 8(2), 45-67. 2016

BRASIL. **Marco Civil da Internet**. Lei 12.965 de 23 de abril de 2014. Diário Oficial da União. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm>. Acesso em 11 de abril de 2024.

BRASIL. **Lei nº 11.419**, de 19 de dezembro de 2006. Código Civil. Diário Oficial da União. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/111419.htm>. Acesso em 29 junho de 2024.

DONEDA, D. O Marco Civil da Internet e a Proteção dos Dados Pessoais. In: **Revista de Direito Constitucional e Internacional**, 22(88), 2014, 120-140.

GAGLIARDI, A. Desinformação e Discurso de Ódio na Internet: Desafios para a Regulação Digital. In: **Revista Brasileira de Estudos Políticos**, 15(1), 2020, pp.90-112.

POLIDO, F., & DONEDA, D. O Processo de Construção do Marco Civil da Internet: Participação Cidadã e Transparência. In: **Revista Direito GV**, 11(2), 2015, pp. 385-406.

RAMOS, Rahellen. **O que é o Marco Civil da Internet?** 2021, Disponível em: <https://www.politize.com.br/marco-civil-da-internet/>. Acesso em: 20 jun 2024;

RODRIGUES, C. Neutralidade da Rede no Brasil: Avanços e Desafios na Implementação do Marco Civil da Internet. In: **Revista de Direito e Tecnologia**, 9(1), 2018, 55-78.

ROCHA, Gustavo. **Ataque hacker ao Tribunal de Justiça do Rio Grande do Sul – TJRS: Efeitos eternos?** Disponível em: usbrasil.com.br/artigos/ataque-hacker-ao-tribunal-de-justica-do-rio-grande-do-sul-tjrs-efeitos-eternos/1268417383. Acesso em 10 jul 2024.

URUPÁ, Marcos. **Dez anos depois, Marco Civil da Internet ainda enfrenta desafios para ser cumprido**. 2024. Disponível em: <https://teletime.com.br/23/04/2024/depois-anos-depois-marco-civil-da-internet-ainda-passa-por-desafios-para-ser-cumprido/>. Acesso em 30 jun. 2024.

MARCO CIVIL DA INTERNET E A TUTELA TRANSVERSAL DOS DIREITOS DA PERSONALIDADE: UM OLHAR SOBRE A PRIVACIDADE NA ERA DA DIGITAL E DE DESAFIOS REGULATÓRIOS INTERNACIONAIS

Daniela Menengoti Gonçalves Ribeiro

Universidade Cesumar (UniCesumar), Paraná.
daniela.menengoti@gmail.com

Adriana Rossini

Universidade Cesumar (UniCesumar), Paraná.
adrianarossini.adv@gmail.com

Resumo: Este artigo investiga a transversalidade da tutela dos direitos da personalidade no ambiente digital, com ênfase na proteção da privacidade, à luz do Marco Civil da Internet (Lei 12.965/2014). A pesquisa parte da seguinte pergunta: como o Marco Civil da Internet pode garantir a proteção dos direitos da personalidade, especialmente a privacidade, diante dos desafios mundiais impostos pela sociedade da informação e dos avanços tecnológicos, como Big Data e Inteligência Artificial? A hipótese sugere que, embora o Marco Civil estabeleça importantes garantias, como a neutralidade de rede e a proteção de dados pessoais, há lacunas regulatórias que comprometem a efetividade da tutela dos direitos da personalidade no ambiente digital. Isso exige uma abordagem mais robusta, transversal e supranacional, levando em consideração que o caráter global da internet requer a criação de marcos regulatórios por meio de tratados internacionais, ao invés de normas exclusivamente nacionais ou de caráter constitucional. O estudo tem como objetivo geral analisar o impacto do Marco Civil da Internet na proteção dos direitos da personalidade, com foco na privacidade, e avaliar como essa legislação pode ser aprimorada para enfrentar os desafios trazidos pelas novas tecnologias. Utilizando o método dedutivo, a pesquisa realiza uma revisão bibliográfica e análise documental, além de examinar a legislação correlata. Conclui-se que, apesar dos avanços proporcionados pelo Marco Civil da Internet, é necessária uma regulação transnacional que assegure uma tutela eficaz da privacidade no ambiente digital. Para tanto, é fundamental que as novas normas regulatórias sejam estabelecidas em um contexto de cooperação internacional, através de tratados, a fim de conciliar o desenvolvimento tecnológico com a proteção dos direitos fundamentais personalíssimos.

Palavras-chave: Marco Civil da Internet; Direitos da personalidade; Privacidade digital; Regulação Internacional; Tutela transversal.

The Brazilian Civil Rights Framework for Internet and the transversal protection of personality rights: a look at privacy in the digital and international regulatory challenges

Abstract: This article investigates the cross-cutting nature of the protection of personality rights in the digital environment, with an emphasis on the protection of privacy, in the light of the Marco Civil da Internet (Law 12.965/2014). The research is based on the following question: how can the Marco Civil da Internet guarantee the protection of personality rights, especially privacy, in the face of the global challenges posed by the information society and technological advances such as Big Data and Artificial Intelligence? The hypothesis suggests that although the

Marco Civil establishes important guarantees, such as net neutrality and the protection of personal data, there are regulatory gaps that compromise the effectiveness of the protection of personality rights in the digital environment. This calls for a more robust, transversal and supranational approach, taking into account that the global nature of the internet requires the creation of regulatory frameworks through international treaties, rather than exclusively national or constitutional standards. The general objective of this study is to analyze the impact of the Marco Civil da Internet on the protection of personality rights, with a focus on privacy, and to assess how this legislation can be improved to meet the challenges brought about by new technologies. Using the deductive method, the research carries out a bibliographical review and documentary analysis, as well as examining related legislation. It concludes that, despite the advances made by the Marco Civil da Internet, there is a need for more specific and comprehensive regulation to ensure effective protection of privacy in the digital environment. To this end, it is essential that the new regulatory standards are established in a context of international cooperation, through treaties, in order to reconcile technological development with the protection of fundamental personal rights. **Keywords:** Marco Civil da Internet; Personality rights; Digital privacy; International regulation; Transversal protection.

INTRODUÇÃO

A era digital trouxe inúmeros desafios para a proteção dos direitos da personalidade, em especial o direito à privacidade. O Marco Civil da Internet (Lei 12.965/2014), criado com o intuito de regulamentar o uso da internet no Brasil, estabeleceu importantes garantias, como a neutralidade de rede e a proteção de dados pessoais. No entanto, o avanço de tecnologias disruptivas, como o *Big Data* e a Inteligência Artificial, impôs novos desafios à eficácia dessa legislação. Diante desse cenário, torna-se essencial reavaliar a capacidade do Marco Civil em assegurar a tutela transversal dos direitos da personalidade, especialmente frente à crescente complexidade das plataformas digitais e o uso massivo de dados pessoais.

Este artigo analisa como o Marco Civil da Internet pode garantir a proteção da privacidade no ambiente digital, considerando os impactos das novas tecnologias e propondo soluções regulatórias para aprimorar a tutela dos direitos fundamentais e de personalidade, adequando-se as diretivas internacionais.

O presente estudo é orientado pela necessidade de compreender como o Marco Civil da Internet pode assegurar a tutela transversal dos direitos da personalidade, com ênfase na proteção do direito à privacidade, diante dos desafios impostos pela sociedade da informação e pelas inovações tecnológicas. Partindo desse problema, a hipótese central sugere que, embora o Marco Civil tenha representado um avanço significativo ao estabelecer garantias fundamentais, ainda há lacunas regulatórias que comprometem a eficácia da proteção dos direitos da personalidade, especialmente no contexto do uso massivo de novas tecnologias.

Para isso, serão explorados objetivos específicos, como: examinar a proteção dos direitos da personalidade no ambiente digital; analisar as disposições do Marco Civil da Internet relacionadas à privacidade; e discutir a necessidade de uma regulação transnacional como resposta eficaz para os desafios apresentados pelas novas tecnologias.

A pesquisa utiliza o método dedutivo, partindo da hipótese de que o Marco Civil necessita de aprimoramentos frente ao avanço tecnológico, e busca, por meio de uma revisão bibliográfica e análise jurídica, comprovar ou refutar essa proposição. Técnicas de pesquisa incluem o levantamento de doutrinas jurídicas, análise de jurisprudência e documentos legais, com o intuito de fornecer uma visão abrangente e crítica sobre o tema.

A pesquisa está estruturada da seguinte forma: inicialmente, contextualiza-se a proteção dos direitos da personalidade no ambiente digital, com foco na privacidade; em seguida, apresenta-se uma análise detalhada do Marco Civil da Internet e suas disposições sobre a proteção de dados; depois, discute-se a transversalidade na tutela da privacidade e os desafios impostos por novas tecnologias, como *Big Data* e inteligência artificial; e, por fim, são propostas melhorias regulatórias para a proteção eficaz dos direitos da personalidade no ambiente digital.

Assim, ao investigar as lacunas e desafios que o Marco Civil da Internet enfrenta na proteção da privacidade frente à crescente globalização digital, este estudo propõe reflexões sobre como uma regulação supranacional pode ser o caminho para assegurar, de forma eficaz, os direitos da personalidade no ambiente digital.

1 MARCO CIVIL DA INTERNET E A PRIVACIDADE

A Lei 12.965/2014, conhecida como Marco Civil da Internet, é uma legislação inovadora no cenário brasileiro e internacional, ao estabelecer um marco regulatório abrangente para o uso da internet no Brasil, tendo como fim máximo, garantir a proteção de direitos fundamentais no ambiente digital. Antes da criação do Marco Civil, a internet no Brasil era regida por leis esparsas, muitas vezes de caráter criminal, e carecia de uma regulamentação que abrangesse os direitos e deveres dos internautas de maneira democrática e organizada. A criação dessa legislação foi um passo fundamental para garantir um uso mais seguro e equilibrado da internet, com a participação ativa da sociedade civil durante seu processo de formulação.

Desenvolvida como uma resposta ao rápido crescimento da internet, que se popularizou na década de 1990, transformou-se em uma ferramenta essencial para o exercício da cidadania, educação, negócios e lazer. Sua criação foi impulsionada pelo reconhecimento da importância de regular os direitos dos usuários e os deveres dos provedores de serviços, estabelecendo um equilíbrio entre a liberdade de expressão e a necessidade de proteção contra abusos no ambiente digital.

Entre os princípios fundamentais do Marco Civil, destacam-se seus três pilares: neutralidade da rede, privacidade e liberdade de expressão. A neutralidade da rede garante que todos os dados trafegados na internet sejam tratados de forma igual, sem discriminação ou cobrança diferenciada por tipo de conteúdo ou serviço. A liberdade de expressão é preservada ao garantir que os usuários possam se manifestar sem medo de censura ou controle indevido. No entanto, um dos maiores avanços dessa legislação está na proteção da privacidade, que se tornou um tema central em tempos de coleta massiva de dados.

A proteção de dados pessoais é uma das maiores conquistas do Marco Civil, refletindo o crescente debate mundial sobre a privacidade dos cidadãos em um ambiente cada vez mais digitalizado. O texto legal impõe obrigações aos provedores de serviço e aplicação no que diz respeito ao tratamento de dados pessoais, exigindo que as informações dos usuários sejam armazenadas de maneira segura e apenas pelo tempo necessário para a prestação de serviços. Além disso, a coleta de dados só pode ocorrer com o consentimento explícito do usuário, o que reforça a importância do controle individual sobre suas informações pessoais.

No entanto, a proteção da privacidade não se limita à segurança dos dados. O Marco Civil também prevê a garantia de que o histórico de navegação dos usuários seja preservado de forma sigilosa, bem como a responsabilização de provedores que falhem em proteger essas informações ou que utilizem os dados coletados para outros fins, sem a devida autorização.

Outro aspecto crucial do Marco Civil da Internet é a definição clara da responsabilidade dos provedores de aplicação e de conexão no que se refere à proteção dos direitos dos usuários. Os provedores de conexão (ou seja, os responsáveis pela oferta de acesso à internet) não podem interferir no conteúdo acessado pelos usuários, assegurando o princípio da neutralidade. Além disso, os provedores de aplicação, como plataformas de redes sociais e serviços de *streaming*, também possuem obrigações legais para proteger os dados dos usuários e devem agir de forma rápida e eficaz para remover conteúdos ilegais ou ofensivos, mediante ordem judicial.

Essa regulamentação é especialmente importante em um contexto onde a privacidade dos usuários pode ser violada por práticas abusivas ou pela exploração comercial indevida de dados pessoais. Assim, o Marco Civil da Internet coloca limites claros sobre como essas informações podem ser coletadas, armazenadas e compartilhadas, exigindo que os provedores garantam a proteção dos direitos fundamentais e personalíssimos no ambiente digital.

O Marco Civil da Internet brasileiro, sem dúvida, marcou um importante avanço na regulação da internet e na proteção dos direitos dos usuários, estabelecendo um alicerce que promove a liberdade de expressão, a segurança jurídica e a privacidade na internet. Além disso, sua relação com a proteção dos direitos da personalidade é evidente, ao garantir a inviolabilidade da intimidade, honra e imagem dos usuários, direitos esses que são fundamentais para a dignidade humana. No entanto, desde sua promulgação em 2014, o cenário tecnológico evoluiu de forma exponencial, trazendo à tona novas ameaças e desafios, como o uso massivo de dados e o crescimento da inteligência artificial. Esses avanços deixam claro que, embora o Marco Civil tenha sido um passo essencial, há uma necessidade urgente de revisitar essa legislação para garantir uma tutela mais robusta dos direitos da personalidade, alinhada aos tratados internacionais de proteção de dados e direitos humanos. A adequação a esses tratados assegura uma proteção transversal, que envolve uma atuação integrada para garantir que as inovações tecnológicas não comprometam os valores fundamentais da personalidade e dignidade humana no ambiente digital.

2 BREVE INTRODUÇÃO AOS DIREITOS DE PERSONALIDADE

O conceito de personalidade tem raízes antigas e profundas, que remontam à Grécia do século IV a.C., onde se deu o início de uma percepção mais acentuada da proteção à personalidade humana. Naquela época, o sentimento de identidade pessoal e sua importância na sociedade começaram a se manifestar de forma mais evidente. Esse movimento continuou a se desenvolver durante o Império Romano, onde se estabeleceram os primeiros passos para o reconhecimento formal da personalidade. Para ser considerado um cidadão com direitos plenos, a pessoa deveria cumprir certos requisitos, como o *status libertatis*, *status civitatis* e *status familiae* (Monteiro, 2007). Aqueles que cumprissem todos esses critérios eram reconhecidos como *caput civile*, e a perda de qualquer um desses atributos resultava em uma *capitis deminutio*, que variava de máxima a mínima, dependendo da gravidade da perda de *status*.

No período medieval, o Cristianismo exerceu uma influência significativa sobre o desenvolvimento da ideia de personalidade, ao promover o ideal de fraternidade universal, que vinculava as noções de bem-estar social e convivência comunitária. Esse ideal de fraternidade permeou o desenvolvimento das constituições e cartas magnas de várias nações, incluindo a Carta Magna inglesa de 1215, que representou um marco importante na admissão dos direitos inerentes ao ser humano (Diniz, 2007).

A evolução do conceito de personalidade avançou ainda mais com a Declaração dos Direitos do Homem e do Cidadão de 1789, que trouxe à tona a valorização dos direitos individuais e da liberdade, fundamentando-se em princípios como igualdade e liberdade de direitos para

todos (Declaração dos Direitos do Homem e do Cidadão, 1789). Este documento estabeleceu bases sólidas para o desenvolvimento posterior dos direitos da personalidade, que foram consolidados ao longo dos séculos seguintes.

Históricamente, o reconhecimento dos direitos da personalidade enfrentou grandes desafios, especialmente devido à confusão entre o sujeito titular dos direitos e o objeto sobre o qual esses direitos se aplicam. Tradicionalmente, esses direitos não foram claramente diferenciados, o que dificultou sua definição e proteção no ordenamento jurídico.

Após o fim da Segunda Guerra Mundial, o impacto devastador causado pelas políticas dos regimes totalitários trouxe à tona a necessidade urgente de proteger a dignidade humana. Foi nesse contexto que a relevância dos direitos da personalidade ganhou destaque no cenário internacional. Documentos importantes, como a Declaração Universal dos Direitos Humanos, aprovada pela Assembleia Geral da ONU em 1948, a Convenção Europeia de Direitos Humanos de 1950 e o Pacto Internacional das Nações Unidas, foram fundamentais para consolidar esses direitos. Esses instrumentos internacionais foram os primeiros passos concretos para o reconhecimento global dos direitos da personalidade, atribuindo-lhes o devido valor no ordenamento jurídico mundial (Diniz, 2017, p. 118-119).

Com o acelerado desenvolvimento tecnológico no período pós-guerra, novas questões emergiram em torno dos direitos humanos. O avanço das tecnologias, além de transformar a vida cotidiana, levou o ser humano a reivindicar um espaço próprio e novos direitos que pudessem refletir as nuances de sua personalidade, agora expostas de maneiras inéditas. No entanto, essas reivindicações não se baseavam em uma perspectiva individualista ou liberal, como ocorrera em períodos anteriores. Em vez disso, o foco passou a ser uma visão mais personalista e ética, que valorizava o desenvolvimento humano e a formação de um ordenamento jurídico capaz de responder às novas demandas sociais.

Os direitos da personalidade envolvem a proteção da integridade física, intelectual e moral dos indivíduos. No aspecto físico, esses direitos incluem a vida, o corpo, os alimentos e o respeito ao corpo vivo ou morto. A integridade intelectual abarca a liberdade de pensamento e a autoria em áreas como a ciência, a literatura e as artes. Já a integridade moral diz respeito à honra, ao segredo profissional e doméstico, à identidade pessoal, familiar e social, além dos direitos autorais (Diniz, 2017, p. 119).

Nesse sentido, a satisfação dessas reivindicações não ocorre pelo mero aumento no número de direitos específicos, mas pela consagração de um direito geral de personalidade. Tal direito serve como uma cláusula geral de proteção à pessoa humana, garantindo os direitos mais essenciais e primordiais. No Brasil, o direito geral de personalidade encontra respaldo tanto no princípio da dignidade da pessoa humana, previsto no artigo 1º, inciso III da Constituição Federal (Brasil, 1988), quanto no artigo 12 do Código Civil, que oferece uma tutela geral dos direitos de personalidade. Esse artigo estabelece que a proteção da personalidade depende da articulação com outros dispositivos legais, como o princípio do solidarismo constitucional (art. 3º, inciso I da CF), garantindo uma defesa abrangente da dignidade individual (Figueiredo, 2013).

A proteção dos direitos de personalidade é uma consequência direta do direito humano à existência digna. A criação de uma cláusula geral de proteção à dignidade humana reflete a necessidade de proteger a pessoa em sua dimensão extrapatrimonial, ou seja, para além dos bens materiais, valorizando sua integridade moral e pessoal. Como bem observa Adriano De Cupis (1961) citado por Saldanha e Oliveira (2022), tem-se como direitos da personalidade: (i) direito à vida e direito à integridade física, (ii) direito à liberdade, (iii) direito à honra e o direito ao resguardo pessoal, (iiii) direito à identidade pessoal e direito moral de autor. Outros doutrinadores também propuseram classificações que, embora tenham pontos semelhantes à apresentada

por De Cupis, divergem quando estabelecem, em um mesmo grupo, direitos que tutelam bens intimamente relacionados. É o caso, por exemplo, do direito à honra e à identidade pessoal.

Assim, os direitos de personalidade e as medidas para sua proteção devem ser analisados caso a caso, com base nas relações jurídicas específicas. É fundamental reconhecer que esses direitos não são exaustivos, pois pertencem ao ser humano por sua própria condição humana. Desse modo, não podem ser limitados a uma lista taxativa, uma vez que continuam a evoluir e a se adaptar às novas realidades sociais e tecnológicas.

Ao longo do tempo, os direitos de personalidade têm sido profundamente vinculados ao princípio da dignidade da pessoa humana, que é a base de todo o sistema de proteção jurídica desses direitos. Esse princípio, consagrado na Constituição de 1988, funciona como uma cláusula aberta, permitindo o surgimento de novos direitos que, embora não expressos diretamente no texto constitucional, derivam da dignidade humana, como é o caso dos direitos humanos.

Consoante Maria Helena Diniz (2017), temos que os direitos da personalidade são absolutos, intransmissíveis, indisponíveis, ilimitados, imprescritíveis e inapropriáveis. Ou melhor, os direitos da personalidade qualificam-se como intransmissíveis e irrenunciáveis, fora do comércio, não podendo o seu exercício sofrer limitação voluntária. Ainda, esses mesmos direitos relativos à integridade física, moral e intelectual da pessoa natural também são inalienáveis e imprescritíveis.

A Constituição Federal de 1988 no Brasil representou um marco contemporâneo na defesa dos direitos da personalidade, ampliando o conceito e reforçando a dignidade da pessoa humana como princípio fundamental (Diniz, 2017). Esse documento, influenciado por marcos históricos como a Declaração Universal dos Direitos Humanos de 1948 e o Pacto Internacional dos Direitos Civis e Políticos da ONU, consolidou a proteção dos direitos da personalidade no contexto jurídico brasileiro.

Atualmente, com o processo de constitucionalização dos diversos ramos do Direito, muito tem se discutido sobre a aplicabilidade dos direitos fundamentais. Entretanto, o significado desses direitos e a importância de sua efetiva aplicação ainda demandam um espaço maior nas discussões jurídicas. É amplamente reconhecido que a promoção desses direitos está diretamente ligada ao fortalecimento das democracias, sendo que a sua proteção e execução são essenciais para o funcionamento do Estado Democrático de Direito (Cunha Júnior, 2016, p. 481).

Os direitos fundamentais, ao serem mencionados, referem-se à proteção de direitos individuais essenciais à sobrevivência humana. Sua eficácia está intimamente relacionada ao desenvolvimento humano, envolvendo a proteção de direitos personalíssimos, que dizem respeito à dignidade, integridade e autonomia de cada indivíduo. A luta histórica por esses direitos reflete o processo contínuo de resistência contra abusos de poder e a busca por um sentido mais profundo para a convivência humana (Siqueira, 2009, p. 9).

Para compreender melhor a questão, é importante conceituar o que se entende por direitos fundamentais. Dirley da Cunha Júnior define-os como todas as posições jurídicas favoráveis às pessoas, as quais, de maneira direta ou indireta, expressam o princípio da dignidade da pessoa humana (Cunha Júnior, 2016, p. 488). Esse conceito é de grande relevância, pois, embora básico, permite a expansão dos direitos fundamentais para novas esferas, como a personalidade digital, que tem se tornado cada vez mais relevante no contexto atual.

Esses direitos possuem *status* constitucional e são de aplicação imediata. A Constituição Federal de 1988 confere-lhes características específicas, como a indisponibilidade e a inalienabilidade, ou seja, não podem ser renunciados ou transferidos. Como aponta Canotilho (1988, p. 30), os direitos fundamentais têm como objetivo assegurar o cumprimento de direitos e atuam

como uma proteção contra o abuso de poder. Do ponto de vista jurídico-objetivo, funcionam como normas de competência negativa, proibindo a interferência arbitrária do Estado na esfera individual dos cidadãos.

Konrad Hesse, citado por Branco (2002, p. 119), ressalta que a efetivação desses direitos depende de vários fatores extrajurídicos, como as peculiaridades culturais e históricas de cada sociedade. Assim, os direitos fundamentais são compreendidos como garantias universais, aplicáveis a todos os indivíduos, independentemente de seu contexto. Nesse sentido, a personalidade digital surge como uma extensão dinâmica desse entendimento, necessitando de reconhecimento, proteção e aplicação imediata, assim como ocorre com os direitos fundamentais no plano tradicional.

3 PROTEÇÃO DOS DIREITOS DA PERSONALIDADE NO AMBIENTE DIGITAL

A globalização, como discutido por Bauman (1999, p. 67), trouxe à tona uma nova dinâmica em que os assuntos globais se tornaram indeterminados e fora de qualquer controle centralizado. A internet, um dos principais motores dessa transformação, permitiu que qualquer pessoa pudesse disseminar informações sem passar por verificações ou processos editoriais, quebrando barreiras e democratizando o acesso à publicação. No entanto, essa liberdade sem filtros também gerou desafios significativos, como a propagação de informações falsas, onde interesses econômicos, políticos ou sociais frequentemente sobrepõem-se à verdade.

Ao mesmo tempo em que a globalização possibilitou que milhões de pessoas tivessem voz e pudessem se expressar livremente, ela também limitou, de certa forma, a capacidade de escolha dos indivíduos. Isso acontece pela manipulação constante de informações a que estão expostos nas redes digitais. As plataformas sociais, diferentemente dos meios de comunicação tradicionais, como jornais, não possuem uma curadoria editorial clara, e o que é publicado é determinado pelas ações e preferências de seus usuários, muitas vezes guiados por algoritmos que amplificam conteúdos sem medir sua veracidade.

Levy (1999, p. 111) compartilha desse pensamento ao enfatizar que o ciberespaço é um universo sem centro e sem uma direção fixa. Ele conecta diferentes pontos e permite que todos sejam participantes e produtores de informação, o que gera um ambiente incontrolável e imprevisível. Essa ausência de controle centralizado no espaço digital teve um impacto profundo nas esferas econômica, política e cultural, alterando as condições da vida em sociedade e tornando o ambiente digital um lugar de grandes repercussões.

Nesse contexto de transformações tecnológicas e globais, torna-se cada vez mais urgente a proteção dos direitos personalíssimos dos indivíduos no ambiente online. A privacidade, a honra e a integridade da pessoa humana, garantidos na vida *offline*, precisam ser igualmente resguardados na esfera digital. As ameaças à liberdade de escolha, à dignidade e à autonomia dos usuários exigem que os mecanismos legais acompanhem a rápida evolução da tecnologia, proporcionando uma proteção robusta e eficaz. Assim, legislações como o Marco Civil da Internet no Brasil surgem como tentativas de equilibrar essa balança, regulando o uso da internet e protegendo os usuários contra abusos que ameaçam seus direitos fundamentais, enquanto apontam para o caminho natural da transnacionalização, ou tutela transversal, necessária para acompanhar as tendências globais de proteção de dados em um ambiente digital cada vez mais interconectado e sem fronteiras.

O entendimento clássico da personalidade civil, que evoluiu conforme o progresso social, ampliou-se para abarcar o que hoje chamamos de “personalidade digital”. Nesse novo ambiente, onde as interações se dão principalmente no espaço virtual, a proteção dos direitos da personalidade torna-se essencial, uma vez que a exposição e a coleta de dados pessoais são constantes (Souza Junior, 2019).

O Marco Civil da Internet exerce um papel fundamental na construção de uma internet mais inclusiva e acessível, assegurando que todos os usuários tenham as mesmas oportunidades de acesso e participação no ambiente digital. Conforme argumentam Souza e De Luca (2015), ao garantir princípios como a neutralidade da rede, a liberdade de expressão e a proteção da privacidade, a legislação promove uma democratização da internet, nivelando as condições de acesso e uso para indivíduos de diferentes realidades sociais e econômicas. Além de promover a igualdade, o Marco Civil tem um impacto significativo na maneira como as interações e relações sociais se formam no mundo digital. De Jesus (2014) aponta que, ao garantir o direito à privacidade e a proteção de dados, a lei estabelece um ambiente mais ético e responsável, onde os direitos e deveres de cada usuário são respeitados. Bitteli (2014) reforça esse ponto ao destacar que o Marco Civil, ao impor diretrizes para o tratamento de dados pessoais nas redes sociais, promove maior transparência e controle sobre as informações compartilhadas, criando uma cultura de confiança entre os usuários. Além disso, o Marco Civil traz segurança jurídica ao definir de forma clara as responsabilidades de usuários, provedores de serviços e intermediários, o que contribui para um ambiente online mais estável e previsível, onde os direitos são protegidos e os abusos, responsabilizados. Assim, a legislação não apenas garante a proteção dos direitos fundamentais no mundo digital, mas também molda um ecossistema mais justo, seguro e democrático para todos.

Ambiente virtual e ambiente físico não são dualismos, mas sim, expressões que compõem o meio ambiente como um todo (Klein, Adolfo, 2022, 56), a proteção desses direitos são cruciais para a construção de um ambiente online mais seguro e democrático, que respeite a dignidade dos indivíduos e os direitos da personalidade, garantindo a conformidade com padrões internacionais de proteção digital. Contudo, o constante avanço tecnológico e a emergência de novas questões, como a inteligência artificial e o tratamento maciço de dados, apontam para a necessidade de aprimoramentos na legislação, assegurando que a proteção da personalidade no meio digital acompanhe as transformações do século XXI.

Outro marco significativo na proteção de dados e privacidade no Brasil foi a promulgação da Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, que estabelece normas para o tratamento de dados pessoais por parte de pessoas físicas e jurídicas. A LGPD (2018) é uma resposta direta às novas demandas da sociedade digital, reconhecendo que os dados pessoais são uma extensão da personalidade e, portanto, precisam ser tutelados de forma eficaz. A lei visa garantir a privacidade, a segurança e a transparência no tratamento de dados, assegurando que os direitos da personalidade sejam respeitados no ambiente digital, seja nas relações comerciais, laborais ou sociais.

Além disso, no plano internacional, a Diretiva Europeia de Proteção de Dados (GDPR) serve de referência ao demonstrar que os direitos da personalidade, incluindo o direito ao esquecimento, à portabilidade de dados e à exclusão de informações pessoais, são essenciais para a proteção dos indivíduos na era digital. A criação de mecanismos jurídicos transnacionais para lidar com os desafios impostos pelas tecnologias digitais é um passo crucial, especialmente diante do poder crescente das grandes empresas de tecnologia (*Big Techs*), que atuam globalmente e muitas vezes colocam em risco os direitos fundamentais.

Nesse sentido, a crescente relevância da personalidade digital impõe a necessidade de uma abordagem multidimensional, que envolve tanto o direito à privacidade e à proteção de dados quanto à integridade moral e à honra, que podem ser violadas de formas até então inimagináveis no mundo *offline*. O ambiente digital facilita ataques à reputação, como os crimes de difamação e calúnia, que se propagam rapidamente através das redes sociais e podem causar danos irreparáveis à imagem e à honra de um indivíduo.

Ademais, no contexto dos direitos da personalidade no ambiente digital, deve-se destacar o direito ao esquecimento, um tema amplamente discutido e que ganha relevância quando se trata da retirada de conteúdos ofensivos ou inadequados da internet. O direito ao esquecimento encontra amparo no princípio da dignidade da pessoa humana e visa a proteger os indivíduos de danos contínuos provocados pela permanência indefinida de informações prejudiciais.

Assim, a proteção dos direitos da personalidade no ambiente digital exige um constante esforço de atualização legislativa e doutrinária, que acompanhe as rápidas mudanças tecnológicas. Nesse sentido, a elaboração de um arcabouço jurídico eficiente e a criação de mecanismos de controle e fiscalização, como as autoridades de proteção de dados, são essenciais para garantir que os direitos da personalidade sejam plenamente respeitados no mundo digital, assegurando que a dignidade humana seja preservada, mesmo diante de inovações tecnológicas contínuas.

Podemos definir a personalidade digital, portanto, como uma extensão inevitável da personalidade civil e jurídica, e sua proteção deve ser abordada com seriedade, diante dos desafios e oportunidades que o ambiente digital oferece.

4 TRANSVERSALIDADE DA TUTELA À PRIVACIDADE: UMA RESPOSTA A DATAFICAÇÃO DA VIDA

A fase de digitalização da cultura digital, que começou a tomar forma na segunda metade do século XX, está agora se transformando em um fenômeno mais abrangente: a dataficação. Este processo consiste na tradução de diversos aspectos da vida cotidiana em dados digitais que são rastreáveis, quantificáveis, analisáveis e performativos. Embora a digitalização continue a desempenhar um papel importante - como na criação de *websites*, na contagem dos passos diários de uma pessoa ou na conversão de livros impressos em e-books - esses processos estão, na verdade, inseridos em algoritmos mais amplos que visam captar e tratar dados, como os que utilizamos em *Big Data* e *machine learning*. A dataficação, portanto, permite a conversão de qualquer ação em dados digitais rastreáveis, produzindo diagnósticos e inferências em uma variedade de domínios (Pessoa *et al*, 2023).

O surgimento da microinformática e da internet, que ocorreu entre as décadas de 1970 e 1990, marcou o início do processo de digitalização. O desenvolvimento das redes sociais, da computação em nuvem e da inteligência algorítmica, por sua vez, acentuou o movimento de dataficação. O estado atual de conversão do mundo em dados remete à origem do que se pode chamar de “culto aos números”, que emergiu nos séculos XVII e XVIII, quando a matemática foi consagrada como modelo de raciocínio e ação útil (Pessoa *et al*, 2023, p. 7). Esse paradigma se tornou o fundamento do discurso que levou à formação da sociedade da informação. Neste sentido, o ambiente virtual constitui um componente intrínseco da realidade social contemporânea. A tutela efetiva do meio ambiente, em todas as suas dimensões, é imperativa (Klein; Adolfo, 2022).

O termo inglês *'datafication'* foi introduzido por Mayer-Schoenberger e Cukier em 2013, referindo-se às maneiras como ações são transformadas em dados quantificáveis, facilitando o

rastreamento amplo e as análises preditivas (Mayer-Schoenberger & Cukier, 2013, p. 28). Essa capacidade de quantificação permite que qualquer ação não apenas seja digitalizada, mas também monitorada com precisão e utilizada para projetar cenários em tempo real ou futuro.

A dataficação vai além da simples conversão de objetos analógicos em digitais; trata-se de uma transformação mais profunda nas ações, comportamentos e conhecimentos que agora são influenciados pela performance dos dados, gerada por sistemas de inteligência algorítmica. Esse fenômeno deve ser compreendido como um conjunto de métodos para coleta, processamento e análise de dados, que permite a realização de previsões sobre comportamentos futuros. A análise não se limita apenas a dados demográficos ou perfis socioeconômicos, mas se expande para uma avaliação dinâmica que considera metadados comportamentais. Isso significa que as decisões e interações humanas estão cada vez mais sendo moldadas por um complexo ecossistema de dados, onde as tecnologias desempenham um papel crucial na interpretação e no direcionamento das nossas ações (Lemos, 2021).

As novas ferramentas tecnológicas, como a Internet das Coisas (IoT) e o *Big Data* (coleta de dados massiva) têm se tornado fundamentais na coleta e armazenamento de uma quantidade imensa de dados dos usuários. Esses dados, considerados a matéria-prima dos algoritmos de Inteligência Artificial, geram preocupações significativas em relação à segurança e à privacidade das informações pessoais.

Essa realidade despertou um crescente interesse dos legisladores em regular a proteção dos dados pessoais, reconhecendo-os como direitos fundamentais dos indivíduos, regidos pelo princípio da não discriminação. Em resposta a essa necessidade, observa-se atualmente um movimento global em direção ao fortalecimento da defesa dos direitos e liberdades dos cidadãos contra os abusos de empresas e governos no que se refere ao controle e ao tratamento de dados pessoais. Esse movimento está cimentando a ideia de uma sociedade mais consciente em relação ao uso e à gestão de dados, conforme destacado por Ferrari *et al.* (2018, p. 06).

À medida que a tecnologia avança, é essencial que a legislação acompanhe essas mudanças, garantindo a proteção dos indivíduos em um ambiente cada vez mais digital e interconectado.

O impacto da transformação digital sobre a privacidade e a coleta de dados pessoais não pode ser subestimado. As grandes empresas de tecnologia, conhecidas como *Big Techs*, como *Google*, *Facebook*, *Apple*, *Amazon* e *Microsoft*, dominam o mercado, detendo cerca de 85% do setor de tecnologia e serviços. O valor econômico dessas organizações, como apontado por Loh (2019), é em grande parte oriundo da análise de dados, que visa não apenas a melhoria da eficiência, mas também o desenvolvimento de produtos inovadores. Em nossa era digital, cada ação realizada online deixa uma marca indelével, refletida nas informações e dados que geramos, formando o que se denomina de pegadas digitais.

Entretanto, essa crescente utilização de dados pessoais e tecnologias como o *Big Data* tem gerado sérios dilemas éticos e controvérsias. Escândalos notáveis, como o da *Cambridge Analytica* em 2018, evidenciam o uso irresponsável de algoritmos e a coleta de dados sem consentimento. A manipulação de informações por meio das redes sociais teve repercussões significativas em eventos políticos, como as eleições de Donald Trump e o referendo sobre o Brexit, demonstrando como a privacidade dos indivíduos pode ser comprometida em um ambiente onde a coleta de dados é amplamente realizada sem a devida supervisão (Lapowsky, 2018).

A vulnerabilidade dos usuários frente a tecnologias complexas é ainda mais alarmante, como evidenciado pela falha de segurança no *Google* em 2020, que afetou milhões de usuários. Nesse contexto, a privacidade online torna-se uma preocupação premente, visto que os dados

podem ser utilizados de forma indevida, levando à manipulação e à criação de perfis comportamentais que influenciam a opinião pública de maneira direta. Os algoritmos, alimentados por dados pessoais, geolocalização e padrões de comportamento, transformam-se em ativos valiosos, utilizados para direcionar publicidade e, em muitos casos, disseminar desinformação.

Em meio a esse cenário de vigilância, tanto o setor público quanto o privado se apropriam das técnicas de monitoramento e classificação. *Startups* e empresas em busca de disrupção também exploram a coleta e o tratamento de dados dos usuários, impactando profundamente as relações sociais. A *Google*, por exemplo, ilustra essa revolução ao se tornar uma das instituições globais mais influentes. A empresa não apenas cataloga informações e desejos, mas transforma esses dados em uma poderosa ferramenta de predição e marketing, influenciando comportamentos e decisões.

Nos primórdios de sua trajetória, a *Google* utilizava dados apenas para aprimorar a experiência do usuário, mas logo percebeu o valor do que Zuboff (2019) chama de “superávit comportamental”. Essa abordagem se traduz na extração e no tratamento de dados, que, independentemente de sua relevância aparente, podem ser convertidos em produtos preditivos e receitas publicitárias. O que temos aqui é o que Zuboff define como um capitalismo de vigilância, que se aproveita da vasta quantidade de dados disponíveis na internet para gerar predições de comportamento, redefinindo a experiência humana como um bem disponível para ser explorado.

Assim, os usuários não são mais considerados meros produtos, mas sim fornecedores valiosos de ativos de vigilância. Esses dados, extraídos das interações dos usuários, tornam-se a matéria-prima para a criação de receitas de vigilância, cujas predições sobre comportamentos e preferências são, em última análise, vendidas para empresas que desejam atuar no mercado comportamental. Nesse cenário, as *Big Techs* emergem como os principais protagonistas de um novo sistema econômico, onde a privacidade e os direitos pessoais estão sob constante ameaça, clamando por uma regulamentação robusta que assegure a proteção do indivíduo em meio a um mar de dados e algoritmos.

Dessa forma, é fundamental observar que essa mudança de paradigma implica uma nova interpretação de conceitos, caracterizada pelo fluxo internacional e transfronteiriço de dados em uma sociedade hiperconectada. Embora tenha se discutido o suposto fim da privacidade no final do século XX, é necessário redefinir o direito à privacidade, superando a visão rígida e estática contida nos textos normativos que promovem o autoconfinamento. Isso requer uma abordagem mais aberta, dinâmica e fluida, adequada a uma sociedade tecnológica (Pessoa *et al*, 2023; Rodotà, 2008).

A proteção da privacidade no ambiente digital é um desafio complexo que envolve múltiplos atores e dimensões, exigindo uma abordagem transversal. A transversalidade, nesse contexto, refere-se à interconexão entre diferentes áreas e agentes, bem como à abrangência da proteção dos direitos, especialmente diante das constantes inovações tecnológicas.

4.1 Conceito de transversalidade na proteção dos direitos de personalidade nas plataformas digitais

A ideia de transversalidade na tutela dos direitos da personalidade, especialmente no que tange à privacidade, implica uma abordagem integrada, em que diferentes setores e normas se sobrepõem e se complementam. Não se trata de uma proteção isolada ou de um único conjunto normativo, mas sim de uma intersecção entre legislações nacionais, internacionais, princípios

constitucionais e regulamentações específicas do ambiente digital. Nesse sentido, a transversalidade garante que a proteção à privacidade envolva uma rede de normas que abranjam diversos campos do direito, como o direito civil, penal, trabalhista e consumerista, além dos direitos humanos.

O caráter supranacional da internet, com sua natureza descentralizada e global, apresenta desafios únicos para a regulamentação por exemplo, das plataformas digitais. As interações *online* transcendem fronteiras geográficas, o que significa que as leis e regulamentos que governam essas interações não podem ser limitados a um único território. Nesse contexto, surge a necessidade de considerar a aplicação extraterritorial das leis de regulação das plataformas digitais, permitindo que as legislações de um país se estendam para além de suas fronteiras nacionais, afetando usuários e serviços em outras jurisdições.

No entanto, essa aplicação extraterritorial deve ser baseada em tratados internacionais entre os Estados, ao invés de depender apenas de normas de caráter constitucional.

Existem inúmeros fatores a serem considerados, como a complexidade normativa e o respeito pela soberania dos países.

As legislações nacionais frequentemente variam significativamente em termos de proteção de dados, direitos autorais, responsabilidade das plataformas e outros aspectos que regem o ambiente digital. Criar marcos regulatórios que possam ser aplicados de maneira uniforme em nível internacional requer um entendimento comum e acordos formais entre os Estados. Somente através de tratados internacionais é possível estabelecer normas que respeitem as diferentes legislações nacionais enquanto proporcionam uma abordagem coesa e eficaz à regulação.

Quanto a soberania estatal, a implementação de normas constitucionais de um único país em outro poderia ser vista como uma violação da soberania. Ao invés disso, tratados internacionais permitem que os Estados concordem mutuamente com as regras que regerão suas interações digitais, respeitando a autodeterminação de cada nação. Isso é particularmente importante em um mundo onde diferentes culturas e sistemas jurídicos coexistem e onde um regulamento imposto unilateralmente pode não ser aceitável ou viável.

A natureza dinâmica da tecnologia e da internet exige que a regulamentação possa evoluir rapidamente em resposta a novas situações e desafios. Tratados internacionais podem incluir cláusulas de revisão e adaptação, permitindo que os países se ajustem às mudanças nas práticas digitais e nas tecnologias emergentes, enquanto normas constitucionais tendem a ser mais rígidas e demoradas para alterar.

A regulação eficaz das plataformas digitais requer colaboração e cooperação entre os Estados. Tratados internacionais promovem o diálogo e a negociação entre países, facilitando a construção de uma governança digital global que é necessária para lidar com problemas como desinformação, violação de dados, e o impacto das plataformas digitais nas democracias.

Outro fator importante a ser analisado é os efeitos e impactos no Comércio Internacional. A regulação das plataformas digitais também tem implicações significativas para o comércio internacional. Normas que se aplicam de forma extraterritorial podem afetar empresas que operam em múltiplas jurisdições. Portanto, a harmonização das regras através de tratados pode evitar a fragmentação do mercado digital e promover um ambiente mais estável e previsível para as empresas que dependem da internet para operar globalmente.

Dessa forma, a construção de marcos regulatórios para plataformas digitais deve ser um esforço colaborativo que transcenda fronteiras, promovendo uma abordagem que respeite as particularidades nacionais enquanto busca garantir a proteção dos usuários e a responsabilidade das empresas em um ambiente digital cada vez mais complexo e interconectado.

4.2 Neutralidade de rede e seus impactos na privacidade

A neutralidade de rede, princípio pelo qual todos os dados que trafegam na internet devem ser tratados de forma igual, sem discriminação de conteúdo, aplicação ou origem, desempenha um papel crucial na preservação da privacidade. Quando esse princípio é violado, surgem riscos à integridade dos dados dos usuários, uma vez que provedores de internet poderiam dar preferência a determinados conteúdos ou restringir o acesso a outros, potencialmente expondo informações pessoais a controle indevido.

A preservação da neutralidade de rede é essencial não apenas para garantir o acesso equitativo à informação, mas também para proteger os dados pessoais de manipulações. Sem essa neutralidade, as plataformas digitais poderiam criar mecanismos que favorecessem certos conteúdos em detrimento de outros, priorizando o lucro e, possivelmente, comprometendo a privacidade e segurança das informações dos usuários.

A transversalidade da tutela à privacidade no ambiente digital exige uma integração entre diferentes normas, atores e princípios que convergem para proteger os direitos da personalidade. Diante das interações complexas com plataformas digitais, redes sociais e sistemas de IA, é essencial que a legislação continue a se expandir e se adaptar, assegurando que a privacidade não seja um conceito ultrapassado, mas sim uma garantia viva e atualizada para todos os cidadãos.

5 DESAFIOS E PERSPECTIVA REGULATÓRIA TRANSNACIONAL

Embora o Marco Civil da Internet tenha sido um marco pioneiro na regulação do ambiente digital no Brasil, ele ainda apresenta algumas lacunas que limitam sua eficácia na proteção dos direitos dos usuários. Uma das principais críticas diz respeito à insuficiência de mecanismos de responsabilização para grandes plataformas tecnológicas, que muitas vezes operam de maneira opaca em relação à coleta e tratamento de dados pessoais. Além disso, o Marco Civil ainda carece de normas mais detalhadas sobre o uso de algoritmos e inteligência artificial, ferramentas amplamente utilizadas pelas *Big Techs*, e que impactam diretamente os direitos da personalidade dos indivíduos. A lei também não aborda de maneira robusta o tratamento de dados sensíveis ou o uso de tecnologias emergentes, como a Internet das Coisas (IoT), que criam novos desafios em termos de privacidade e segurança de informações.

Dado o caráter supranacional da internet e a atuação global das grandes plataformas digitais, torna-se imperativa a criação de uma regulação que vá além das fronteiras nacionais. A internet opera de maneira transfronteiriça, o que faz com que os efeitos de decisões regulatórias de um país impactem diretamente outros territórios. Nesse contexto, tratados internacionais e marcos regulatórios globais são essenciais para criar um ambiente digital mais seguro e coeso. A ausência de um quadro regulatório internacional coordenado pode resultar em uma “corrida para o fundo do poço”, em que as empresas buscam operar em jurisdições com regulamentações mais fracas, fragilizando ainda mais a proteção dos dados e da privacidade. Iniciativas como o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia mostram a importância de uma regulamentação sólida, que, ao ser aplicada extraterritorialmente, impõe normas mais

Marco Civil da Internet e a tutela transversal dos direitos da personalidade: um olhar sobre a privacidade na era da digital e de desafios regulatórios internacionais

rígidas em nível global. No entanto, ainda há desafios significativos para harmonizar as diferentes abordagens regulatórias adotadas por países com visões distintas sobre privacidade, liberdade de expressão e neutralidade da rede.

Para aprimorar a proteção dos direitos da personalidade no ambiente digital, é necessário que a legislação se adapte rapidamente às novas tecnologias e práticas adotadas pelas plataformas digitais. Uma das propostas mais urgentes envolve o estabelecimento de regras claras e transparentes para o uso de algoritmos, especialmente no que tange à coleta de dados, criação de perfis e tomada de decisões automatizadas. A introdução de mecanismos de auditoria e transparência nos sistemas de IA poderia ajudar a mitigar os riscos associados a decisões enviesadas e invasivas. Além disso, é preciso incentivar uma maior cooperação internacional para desenvolver normas transnacionais de proteção de dados, estabelecendo um padrão global de privacidade que garanta aos indivíduos maior controle sobre suas informações, independentemente da jurisdição em que os dados estejam sendo processados. Finalmente, deve-se promover o fortalecimento da educação digital para que os usuários compreendam melhor os riscos e direitos associados ao uso de suas informações na internet, capacitando-os a navegar de forma mais consciente e segura no ambiente digital.

CONCLUSÃO

A proteção dos direitos da personalidade, especialmente a privacidade, tornou-se um tema premente na era digital, em que as *Big Techs* exercem um controle significativo sobre os dados pessoais dos usuários. O Marco Civil da Internet, embora represente um avanço legislativo importante, enfrenta o desafio de garantir a efetividade dessa proteção diante da complexidade e da interconectividade das novas tecnologias. Para que a tutela dos direitos da personalidade seja realmente eficaz, é crucial que a regulação se adapte às realidades impostas por essas empresas, que operam em um espaço global.

O poder das *Big Techs* sobre dados pessoais não se limita à coleta e ao armazenamento de informações; ele afeta diretamente direitos fundamentais como a privacidade, o direito à imagem, ao nome e à intimidade. A regulação transnacional deve se concentrar não apenas em questões econômicas, mas também em garantir que essas empresas respeitem os direitos da personalidade em todas as jurisdições em que atuam. A proteção da privacidade deve ser um direito inalienável, e a responsabilidade das empresas em relação ao tratamento de dados pessoais deve ser universalmente reconhecida.

Para tanto, deve-se levar em consideração o impacto que as *Big Techs* exercem nos direitos de personalidade, uma vez que a coleta e o uso de dados pelas *Big Techs* frequentemente violam os direitos da personalidade. Tecnologias como algoritmos e reconhecimento facial têm o potencial de comprometer a identidade e a autonomia individual, criando cenários em que o indivíduo se torna um mero objeto de exploração comercial. A falta de uma regulação adequada e robusta em escala global agrava essa situação, colocando em risco não apenas a privacidade, mas a dignidade humana em seu conjunto. É necessário, portanto, um enfoque regulatório que proteja os direitos de personalidade de forma integral e preventiva.

Não faltam documentos e diálogos focados atualmente na governança da IA. Governos, empresas e consórcios, bem como organizações internacionais e regionais, adotaram centenas de diretrizes, marcos e princípios. São inúmeros os fóruns que reúnem atores, desde processos intergovernamentais estabelecidos e organismos especializados até iniciativas ad hoc de múltiplas partes interessadas, no entanto, a criação de um regime regulatório transnacional é imperativa para a proteção dos dados pessoais e dos direitos da personalidade.

O conceito de *Lex Digitalis* deve ser ampliado para englobar não apenas normas técnicas, mas também princípios éticos que assegurem a dignidade e os direitos dos indivíduos no ambiente digital. A harmonização das legislações em diferentes países pode facilitar a criação de um padrão global de proteção, garantindo que os direitos da personalidade sejam respeitados independentemente da localização da empresa ou do usuário.

A relação entre a soberania dos Estados e a proteção dos direitos da personalidade merece especial atenção. A crescente influência das *Big Techs* pode enfraquecer a capacidade dos Estados de proteger seus cidadãos, especialmente no que diz respeito à privacidade e ao uso indevido de dados pessoais. É fundamental que os Estados reavaliem suas estratégias regulatórias, buscando formas de exercer controle sobre essas plataformas e de garantir a proteção dos direitos de seus cidadãos, independentemente da origem das empresas envolvidas.

Em conclusão, a efetividade da tutela dos direitos da personalidade no contexto digital requer uma abordagem integrada e holística. O Marco Civil da Internet, embora seja um passo importante, deve ser constantemente aprimorado para acompanhar as transformações tecnológicas e sociais que caracterizam a sociedade da informação.

A transversalidade se revela como um elemento essencial na proteção e efetivação dos direitos de personalidade, especialmente no que tange à privacidade, em um mundo digital cada vez mais interconectado. Este conceito propõe que a proteção da privacidade não deve ser vista como uma questão isolada, mas sim integrada a uma variedade de contextos, incluindo a legislação, a tecnologia, a ética e a educação. Ao adotar uma abordagem transversal, garantimos que a privacidade permeie todas as práticas e políticas que envolvem o tratamento de dados pessoais, assegurando que os direitos da personalidade sejam respeitados em todas as esferas da sociedade.

Nesse sentido, a legislação vigente, como o Marco Civil da Internet, precisa ser aplicada de forma coesa e integrada com outras normas, como as que abordam direitos do consumidor e proteção de dados. Essa sinergia não só facilita a compreensão das disposições legais, mas também fortalece a proteção dos direitos individuais, mesmo diante de contextos onde interesses diversos possam conflitar. Além disso, o avanço das tecnologias emergentes, como a inteligência artificial e o *Big Data*, exige que desenvolvedores e empresas considerem cuidadosamente as implicações de suas inovações sobre a privacidade. Ao projetar sistemas e algoritmos, é fundamental que a privacidade seja uma prioridade, garantindo que as soluções tecnológicas respeitem a dignidade humana.

Outro aspecto importante da transversalidade é a promoção da educação e conscientização sobre a privacidade como um direito fundamental. É imprescindível que iniciativas educativas sensibilizem os usuários para a importância da proteção de seus dados pessoais, capacitando-os a tomar decisões informadas. Uma abordagem educativa integrada, que inclua direitos digitais e privacidade nos currículos escolares e em campanhas de conscientização, contribui para o empoderamento dos indivíduos em relação ao seu próprio espaço digital.

Por fim, a natureza global da internet torna a colaboração internacional uma necessidade inadiável. As *Big Techs* operam em múltiplas jurisdições, e a criação de tratados e acordos internacionais pode facilitar a implementação de normas comuns, garantindo a proteção dos direitos da personalidade em todo o mundo. Essa cooperação é vital para enfrentar as lacunas regulatórias existentes e promover uma governança digital que respeite a privacidade, independentemente da localização.

A transversalidade não apenas fortalece a proteção da privacidade, mas também é crucial para a efetivação dos direitos de personalidade em uma sociedade digital. Ao integrar a proteção

Marco Civil da Internet e a tutela transversal dos direitos da personalidade: um olhar sobre a privacidade na era da digital e de desafios regulatórios internacionais

da privacidade em legislações, práticas tecnológicas, educação e esforços internacionais, podemos construir um ambiente digital que respeite e promova os direitos dos indivíduos.

A responsabilidade recai tanto sobre as autoridades regulatórias quanto sobre as empresas que operam nesse espaço, sendo imperativo que ambas atuem em conjunto para garantir que o avanço tecnológico não comprometa os direitos fundamentais personalíssimos dos indivíduos. Assim, é possível construir uma sociedade digital mais justa, equitativa e consciente.

REFERÊNCIAS

BRANCO, Paulo Gustavo Gonet. Aspectos de teoria geral dos direitos fundamentais. *In*: MENDES, Gilmar Ferreira et al. **Hermenêutica e direitos fundamentais**. Brasília: Brasília Jurídica, 2002.

BRASIL. **Código Civil**. 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/110406compilada.htm. Acesso em: 27 set. 2024.

BRASIL. **Lei geral de proteção de dados pessoais**. 2018. Disponível em:

http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 27 set. 2024.

BRASIL. **Declaração dos direitos do homem e do cidadão de 1789**. Disponível em:

<https://www.ufsm.br/app/uploads/sites/414/2018/10/1789.pdf>. Acesso em: 27 set. 2024.

BRASIL. **Constituição da República Federativa do Brasil**, de 5 de outubro de 1988.

Disponível em: www.senado.gov.br/sf/legislacao/const. Acesso em: 27 set. 2024.

BRASIL. **Código Civil**. Lei nº 10406, de 10 de janeiro de 2002. Disponível em:

www.senado.gov.br/sf/legislacao/const. Acesso em: 27 set. 2024.

CANOTILHO, J. J. G. **Direito constitucional e teoria da constituição**. 7ª edição. Coimbra: Almedina, 2010.

CUNHA JÚNIOR, Dirley Da. **Curso de direito constitucional**. Salvador: JusPODIVM, 2016.

CUPIS, Adriano de. **Os direitos da personalidade**. Lisboa: livraria morais, 1961.

DE JESUS, Damásio. **Marco Civil da Internet**: comentários à Lei n. 12.965, de 23 de abril de 2014. Saraiva Educação SA, 2014.

DINIZ, Maria Helena. **Curso de Direito Civil Brasileiro**. São Paulo: Saraiva, 2017.

FERRARI, Isabela; BECKER, Daniel; WOLKART, Erik Navarro. Arbitrium ex machina: panorama, riscos e a necessidade de regulação das decisões informadas por algoritmos. **Revista dos Tribunais**, v. 995, 2018. Disponível em: <https://bdjur.stj.jus.br/jspui/handle/2011/125801>. Acesso em: 27 set. 2024.

FIGUEIREDO, Fábio Vieira. **Direitos da personalidade e o respeito à dignidade da pessoa humana**. Texto Digital, 2013. Disponível em: <chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://ibdh.org.br/wp-content/uploads/2016/02/Book-O-respeito-%C3%A0-dignidade-da-pessoa-humana.jpg.pdf>

Acesso em: 27 set. 2024.

KLEIN, Júlia; ADOLFO, Luiz. A nuvem digital e a ameaça invisível ao direito fundamental ao meio ambiente na sociedade da informação. **Revista Jurídica da FA7**, [S. l.], v. 19, n. 1, p. 51–62, 2022. DOI: 10.24067/tjfa7;19.1:1251. Disponível em: <https://periodicos.uni7.edu.br/index.php/revistajuridica/article/view/1251>. Acesso em: 25 set. 2024.

LAPOWSKY, Isse. **How Cambridge Analytica sparked the great privacy awakening**. Wired. São Francisco: 17 mar 2018. Disponível em:

<https://www.wired.com/story/cambridge-analytica-facebook-privacy-awakening/>. Acesso em: 27 set. 2024.

LEMOS, André. Dataficação da vida. **Civitas: revista de Ciências Sociais**, [S. l.], v. 21, n. 2, p. 193–202, 2021. DOI: 10.15448/1984-7289.2021.2.39638. Disponível em: <https://revistaseletronicas.pucrs.br/civitas/article/view/39638>. Acesso em: 27 set. 2024.

LEVY, Pierre. **Cibercultura**. Tradução de Carlos Irineu da Costa. São Paulo: Editora 34, 1999.

LOH, Stanley. Volume, Velocidade, Variedade, Veracidade e Valor: Como os 5 Vs do Big Data estão impactando as Organizações e a Sociedade. Porto Alegre, 2019. Disponível em:

<https://www.intext.com.br/5vs-big-data.pdf>. Acesso em: 27 set. 2024.

ONU. Assembléia Geral das Nações Unidas. Declaração Universal dos Direitos Humanos, 1948. Disponível em: http://www.mj.gov.br/sedh/ct/legis_intern/ddh_bib_inter_universal.htm. Acesso em: 27 set. de 2024.

PESSOA, João Pedro Seefeldt; SALDANHA, Jânia Maria Lopes; LIMBERGER, Têmis. A proteção de dados pessoais entre capitalismo de vigilância e cosmopolitismo. **Revista da Faculdade Mineira de Direito - PUC Minas**, v. 26 n. 52 (2023). DOI: <https://doi.org/10.5752/P.2318-7999.2023v26n52p156-185>. Acesso em: 27 set. de 2024.

RODOTÀ, Stefano et al. A vida na sociedade da vigilância: a privacidade hoje. In: **A vida na sociedade da vigilância: a privacidade hoje**. Rio de Janeiro; Renovar, 2008. p. 381-381.

SALDANHA, Rodrigo Róger; OLIVEIRA, José Sebastião de. A quarta expressão dos direitos de personalidade: o conjunto informativo digital como um novo conceito no Direito Civil contemporâneo. **Revista Húmus**, v. 12, n. 37, 13 Dez 2022. Disponível em:

<https://cajapio.ufma.br/index.php/revistahumus/article/view/19182>. Acesso em: 27 set 2024.

SIQUEIRA, Dirceu Pereira; PICCIRILLO, Miguel Belinati. **Direitos fundamentais: a evolução histórica dos direitos humanos, um longo caminho**. Rio Grande: Âmbito Jurídico. 2009.

SOUZA JUNIOR, Arthur Bezerra de; GOMES, Daniel Machado; FAÇANHA, Josanne; SILVA, Leonardo Rabelo de Matos da (orgs.). **Direito privado contemporâneo**. 2. ed. Rio de Janeiro: FGV / Pembroke Collins, 2019.

SOUZA, Lucas Daniel Ferreira; DE LUCA, Guilherme Domingos. Lei 12.965/2014: democratização da internet e efeitos do marco civil na sociedade da informação. **Revista Paradigma**. [S. l.], n. 23, 2015. Disponível em: <https://revistas.unaerp.br/paradigma/article/view/466>.

TEPEDINO, Gustavo. **A tutela da personalidade no ordenamento civil: constitucional brasileiro**. In: Temas de direito civil. Rio de Janeiro: Renovar, 1999.

ZUBOFF, Shoshana. **The Age of Surveillance Capitalism: the fight for a human future at the new frontier of power**. Nova York:Public Affairs, 2019.

O MARCO CIVIL DA INTERNET E A DOCTRINA DO DIÁLOGO DAS FONTES

Rogério da Silva e Souza

Universidade Federal Rural do Semi-Árido (UFERSA), Rio Grande do Norte.

rogeriojur75@gmail.com

Resumo: A pesquisa explora se fundamenta na doutrina do diálogo das fontes, propondo uma reflexão crítica sobre a interação normativa para enfrentar os desafios da proteção de dados no Brasil, exigindo uma interação efetiva entre o Marco Civil da Internet, a Lei Geral de Proteção de Dados e o Código de Defesa do Consumidor, cujo objeto de estudo é investigar como o diálogo entre essas legislações, analisando a problemática da (in)disponibilidade desses direitos em um contexto de autodeterminação informacional e liberdade humana. A metodologia empregada é exploratória, com análise bibliográfica e doutrinária, além da consulta a decisões judiciais. Destaca-se que o Marco Civil da Internet, embora celebrado como um marco regulatório enfrenta limitações para garantir segurança jurídica no tratamento de dados, nesse contexto, a Lei Geral de Proteção de Dados surge como resposta à necessidade de uma cultura de privacidade e o Código de Defesa do Consumidor a garantir princípios nas relações de consumo mediadas por plataformas digitais, há ainda dilemas éticos e jurídicos, como a tensão entre liberdade de expressão e responsabilidade pelo uso de dados, exemplificada pela incapacidade de instituições protegerem ambientes online, especialmente de grupos vulneráveis, como crianças. Para tanto, considerando o diálogo entre Marco Civil da Internet, L Lei Geral de Proteção de Dados e Código de Defesa do Consumidor é considerável transcender a mera conformidade legal, promovendo uma abordagem que combine liberdade informacional com segurança de dados.

Palavras-chave: Direitos Privado. Marco Civil da Internet. Lei Geral de Proteção de Dados. Código de Defesa e Proteção do Consumidor. Proteção de Dados

The Brazilian Civil Rights Framework for the Internet and the doctrine of the dialog of sources

Abstract: The research is based on the doctrine of the dialogue of sources, proposing a critical reflection on the normative interaction to face the challenges of data protection in Brazil, requiring an effective interaction between the Civil Rights Framework for the Internet, the General Data Protection Law and the Consumer Protection Code, whose object of study is to investigate how the dialogue between these legislations, analyzing the problem of the (un)availability of these rights in a context of informational self-determination and human freedom. The methodology employed is exploratory, with bibliographical and doctrinal analysis, as well as consultation of court decisions. It is noteworthy that the Brazilian Civil Rights Framework for the Internet, although celebrated as a regulatory framework, faces limitations in guaranteeing legal certainty in the processing of data. In this context, the General Data Protection Law emerges as a response to the need for a culture of privacy and the Consumer Protection Code to guarantee principles in consumer relations mediated by digital platforms, there are also ethical and legal dilemmas, such as the tension between freedom of expression and responsibility for the use of data, exemplified by the inability of institutions to protect online environments, especially vulnerable groups such as children. To this end, considering the dialogue between the Brazilian Civil Rights Framework for the Internet, the General Data Protection Law and the Consumer Protection Code, it is considerable to transcend mere legal compliance, promoting an approach that combines informational freedom with data security.

Keywords: Private Rights. Civil Rights Framework for the Internet. General Data Protection Law. Consumer Protection Code. Data Protection

INTRODUÇÃO

É conhecida a doutrina do diálogo das fontes com destaque no pensamento de Erik Jayme, saudoso professor da Faculdade de Direito da Universidade de Heidelberg, Alemanha, falecido em 2 de maio de 2024; no Brasil com os recortes e adaptações introduzidas por Cláudia Lima Marques,¹ é hoje, outrossim, aporte teórico para a concretização de método hermenêutico.²

No atual cenário um desafio para os institutos afins, a saber, Marco Civil da Internet (MCI – Lei 12.965/14) Lei Geral de Proteção de Dados (LGPD – Lei 13.709/2018) e Código de Defesa do Consumidor (CDC – Lei 8.078/91), daí as mudanças que hão de vir nas reformas do código consumerista e também a forma dialogada que deve haver nas legislações contemporâneas.

Em linhas gerais, enquanto as ideologias político-econômicas debatem entre a preservação do patrimônio tecnológico e a redistribuição de recursos informáticos, o MCI preocupa-se com a orientação da justiça sobre a rede mundial de computadores, por essa ordem, a função legislativa dos Estados legisladores é libertar a legislação do exclusivismo ideológico associado a polarizações sociais; promovendo uma abordagem que seja tanto econômica quanto moral em torno da justiça para a internet, uma espécie de interpretação autêntica perante as novas dimensões sociais, e com o impacto da globalização.³

Com o impacto crescente das tecnologias, os avanços se tornam cada vez mais evidentes, dando origem a estudos relacionados ao conceito da “quarta revolução industrial”, contudo, a questão central não reside nas tecnologias já existentes para contemporizar os direitos, pois essas são categorias que já foram ou estão sendo implementadas, pois o verdadeiro desafio reside em questionar se o futuro dos direitos será determinado ou não pela experiência humana sem a autonomia praticamente autônomo das redes, mas, é imperativo que a ausência humana não determine os caminhos dos direitos, e por essa forma, novas instituições ou atualizações surgiram nas instituições de direito como é o caso da LGPD e das propostas reformistas do CDC sob o intuito da proteção das pessoas *in favor debilis*.

O conto *A Nova Roupa do Rei* de Hans Christian Andersen, há muito, narra a história de um monarca enganado por tecelões desonestos que o convencem de estar usando uma roupa invisível, quando na verdade está completamente nu; sob uma metáfora contemporânea, revela-

¹ Neste sentido vide MARQUES, Cláudia Lima Marques (coord.). *Diálogo das fontes: do conflito à coordenação das normas de direito*. São Paulo: Revista dos Tribunais, 2012.

² A teoria do diálogo das fontes foi aplicada pela primeira vez no Supremo Tribunal Federal (STF) no julgamento da ADI 2.591/2006, de relatoria do Ministro Joaquim Barbosa. Na ocasião, discutia-se a constitucionalidade da Lei nº 9.637/1998, que dispõe sobre as Organizações Sociais. Em sua ementa, o ministro destacou a necessidade de harmonizar normas constitucionais e infraconstitucionais para assegurar os princípios fundamentais, apontando que a “interpretação sistemática exige a leitura conjunta e coordenada de diferentes normas, para evitar contradições ou conflitos entre elas”. Este julgamento consolidou a aplicação do diálogo das fontes como método interpretativo no STF. Neste sentido, vide o STF na ADI 2.591 Rel. Min. Joaquim Barbosa a entender pela incidência do CDC às atividades bancárias., em franca disposição do diálogo das fontes.

³ É preciso destacar antes as pessoas em primeiro lugar, que Amartya Sen e Bernardo Kliksberg (2010, p.23) em livro homônimo adverte quanto ao problema humano na era tecnológica, a saber: “De fato, não podemos reverter as dificuldades econômicas dos pobres no mundo se impedirmos que eles tenham acesso às grandes vantagens da tecnologia contemporânea, à bem estabelecida eficiência do comércio e do intercâmbio internacionais e aos méritos sociais e econômicos de viver em uma sociedade aberta. Na verdade, o ponto central é como fazer um bom uso dos formidáveis benefícios do intercuro econômico e do progresso tecnológico de maneira a atender de forma adequada aos interesses dos destituídos e desfavorecidos.”

se pertinente atribuir-se aos comandos da rede mundial de computadores, quando se discute a efetividade do Marco Civil da internet na proteção dos dados no Brasil, pois apesar de seu objetivo de regular o uso da internet e garantir direitos fundamentais no âmbito digital, o instituto *per si* é insuficiente em proporcionar a segurança necessária aos dados das pessoas deixando-as tão expostas quanto o rei da literatura de Andersen?

O MCI foi celebrado como um avanço significativo na regulação do uso da internet no Brasil, estabelecendo princípios, garantias, direitos e deveres para usuários e provedores e a proteção de dados, que deveria ser uma das peças centrais dessa "nova roupa" jurídica, revela-se pífia diante dos desafios contemporâneos impostos pela rápida evolução tecnológica, nas relações de consumo virtuais e pelo uso intensivo de informações pessoais por empresas e plataformas digitais.⁴

O instituto do MCI é uma norma que mostra que a humanidade preferiu prevenir danos, antes de reparar, dado o grau acentuado das transformações que refletem as dimensões dos direitos fundamentais, sobretudo, quanto aos direitos de personalidade e a implementação prática dessa legislação ainda enfrenta desafios significativos, como a falta de uma cultura consolidada de privacidade e proteção de dados entre os sujeitos sociais e as empresas, além de enfrentamentos na fiscalização e aplicação dessas normas.

Nesta ordem, propõe-se uma reflexão crítica sobre o estado atual da proteção de dados no Brasil, argumentando que, assim como no conto de Andersen, a roupa jurídica fornecida pelo MCI e o diálogos das fontes com a LGPD e com o CDC há de minimizar os efeitos da insuficiência jurídica, explorando-se o debate entre os institutos para a proteção dos dados pessoais das pessoas na grande rede, garantindo-se que os direitos fundamentais sejam resguardados em um ambiente digital cada vez mais complexo e dinâmico.⁵

Essa discussão perpassa o MCI, fazendo contrapor o direito à liberdade de comunicação e autodeterminação pessoalíssima nas redes sociais, sugerindo-se a seguinte problemática da pesquisa: como se dá a afirmação das fontes dialogadas, da LGPD e do CDC, para a proteção das pessoas na era tecnológica em face do MCI? E tal questionamento leva a crer a (in)disponibilidade dos direitos de personalidade em tempos de autodeterminação dos direitos, ou seja, aonde se quer chegar ou limitar o estado da tecnologia em virtude da liberdade humana.

A metodologia traduz-se por uma abordagem livre e exploratória em torno da temática, compreendendo os fundamentos críticos em torno da doutrina do diálogo das fontes, e ainda é

⁴ Diante dessa nova realidade de dados Lévy assinala: “Essas verdadeiras usinas informacionais – o novo *hardware* da informática nas nuvens – reúnem centenas de milhões de computadores interconectados em prédios sob alta vigilância, que consomem a energia de pequenas centrais elétricas. Na prática, o imenso domínio em expansão da memória mundial em rede é, portanto, explorado por ‘computadores centrais’ de um novo gênero. Dispersos no mundo para ficarem mais próximos da demanda, esses centros de cálculo estão diretamente conectados nos canais principais da Internet e são capazes de tratar massas vertiginosas de informação.” LÉVY, Pierre. *A esfera semântica*. Tomo I: computação, cognição e economia da informação. São Paulo: Annablume, 2014. (Coleção Atopos). pp.402-403.

⁵ Fernanda Borghetti Cantali assegura: “[...] o impacto que a revolução tecnológica vem causando também diz com o direito à privacidade, principalmente em função da *internet* e o seu fluxo de troca de informações. Em legítimo ato de disposição de privacidade, as pessoas, por vontade própria, relatam suas vidas em diários eletrônicos, os *Blogs*, disponibilizam vídeos, inclusive de cenas mais íntimas, em sites como o *Youtube*, descrevem seu perfil em *sites* de relacionamento como o *Orkut*, permitem a filmagem de sua vida íntima em tempo real através de *webcams*, sem falar naqueles que ingressam no fenômeno mundial de audiência *Big Brother*, situação em que os indivíduos têm a sua privacidade completamente suprimida, transmitindo ao vivo o cotidiano das pessoas. Os novos recursos tecnológicos abriram um leque de possibilidades, mas as revistas que se destinam a mostrar a vida privada de pessoas famosas e as biografias autorizadas são exemplos de práticas completamente incorporadas na sociedade.” CANTALI, Fernanda Borghetti. Direitos da personalidade: disponibilidade relativa, autonomia privada e dignidade humana. Porto Alegre: Livraria do Advogado, 2009. p.196;

do tipo bibliográfica na afirmação de literatura jurídica especializada, decisões judiciais para o manifesto referencial teórico do estudo.

Para tanto, na primeira parte do estudo vê-se a proteção de dados, inserida no contexto dos direitos fundamentais, revelando-se com uma questão complexa na era digital, onde a interação entre tecnologia e sociedade demanda uma análise crítica; utiliza-se do dilema, enquanto exemplo, das crianças em um recreio virtual, no qual ofensas e discriminações emergem, expõe a incapacidade das instituições de garantir um ambiente seguro online, refletindo a dificuldade em lidar com os desafios éticos e legais dessa nova realidade, cuja situação ilustra a necessidade de considerar os direitos de proteção de dados como parte de uma nova dimensão dos direitos fundamentais, onde o direito à informação, à privacidade e à integridade moral se tornam centrais.

Na sequência, exploram-se os princípios de proteção de dados estabelecidos no Marco Civil da Internet, na Lei Geral de Proteção de Dados e no Código de Proteção de Defesa do Consumidor, reconhecidos como fundamentais para orientar a aplicação das normas jurídicas em cenários complexos, destacando-se o dilema entre a liberdade de expressão e a responsabilidade pelo tratamento de dados.

Por último, evidencia-se que embora MCI, LGPD e CDC façam significativas implementações no cenário jurídico, ao mesmo enfrentam desafios diante da rápida evolução tecnológica e da complexidade inerente ao equilíbrio entre liberdade e segurança informacional, destarte, o diálogo das fontes entre os institutos em evidencia sob a necessidade de uma abordagem mais profunda e reflexiva na proteção dos dados pessoais, transcendendo a mera conformidade legal.

1 A PROTEÇÃO DE DADOS E OS DIREITOS FUNDAMENTAIS

Para fomentar a discussão utiliza-se da seguinte narrativa introdutória⁶: um grupo de crianças, durante o recreio em uma aula remota, desviou-se dos temas escolares e começou a trocar palavras que logo se transformaram em ofensas. As discussões foram além do aceitável, com ataques à condição econômica, crenças religiosas e cor de pele dos colegas.

Diante desse cenário, a direção da escola decidiu cancelar o recreio remoto, o que gerou descontentamento entre os alunos, levando-os a relatar a situação aos pais, estes por sua vez indignados passaram a exigir que a escola restabelecesse o recreio, argumentando que, no ambiente físico, as crianças têm o direito de interagir, mesmo que eventualmente surjam conflitos; a escola, no entanto, esclareceu que o problema ia além das ofensas: tratava-se de sua incapacidade de garantir um ambiente virtual seguro, já que ainda não estava preparada para os desafios que essa nova modalidade de ensino impõe.

A ideia proposta na situação hipotética se revela complexo, pois é engendrada por um pensamento sistêmico, relacionando-se em pelo menos duas categorias, a saber: a proteção da personalidade dos infantes em ambiente virtual e a gravação/disposição das falas e das imagens em dados em sala de aula remota. A escola aqui é a representação de qualquer corporação econômica e sua funcionalidade com as redes, a expressar a reflexão de Sennett (2008, p. 52-53):

⁶ A narrativa apresentada foi disposta sob a denominação “do complexo recreativo dos alunos em ambiente virtual em SOUZA, Rogério da Silva e; ROCHA, Maria Vital da. Os direitos de personalidade na era tecnológica em especial à lei geral de proteção de dados. In: Etiene Luiza Ferreira Pleti; Heloisa Helena de Almeida Portugal; Jefferson Patrik Germinari. (Org.). Direito Digital e Desenvolvimento: olhares transdisciplinares sobre a efetivação de direitos. 1a.ed.Uberlândia: LAECC, 2022, v. . p. 231-246.

“Novas tecnologias de análise têm permitido às empresas promover o que Michel Foucault chamava de ‘vigilância panóptica’; são tecnologias que projetam na tela mapas de recursos e desempenho em tempo real”.⁷

A concepção de que a rede mundial de computadores arbitra a experiência humana dos direitos é uma falácia que requer uma análise crítica das interações entre tecnologia e sociedade. Assim como o mercado é um sistema de trocas que a economia estuda para melhorar a produção de bens, a tecnologia, em particular a internet, não é necessariamente a causa ou o objetivo final das ações humanas.⁸

Em uma sociedade digital, há reflexos práticos que incidem sobre a proteção de dados. Não é oportuno dizer que a proteção de dados pessoais estão dispostos somente no âmbito dos direitos de primeira dimensão (liberdade), posto que podem ainda ser vistos, à perspectiva de dados pessoais, como direitos de quarta dimensão. Para a boa doutrina, é possível entender esses direitos, no âmbito das dimensões de direitos fundamentais, a saber, os de quarta dimensão, na esteira dos direitos à informação como pensa, *verbi gratia*, o constitucionalista Bonavides (2017, p. 586):

São direitos da quarta dimensão o direito à democracia, o direito à informação e o direito ao pluralismo. Deles depende a concretização da sociedade aberta do futuro, em sua dimensão de máxima universalidade, para a qual parece o mundo inclinar-se no plano de todas as relações de convivência.

Quando a *General Data Protection Regulation* (GDPR) surgiu na comunidade europeia, oriunda das legislações do último quartel do século XX, não deveria ser motivo de novidade a protagonização de direitos fundamentais às Cartas políticas mundiais, todavia era inoportuna a forma pela qual o mercado tecnológico fazia-se avançar no trato econômico sobre os dados das pessoas, neste sentido adverte Lévy (1987, p. 38):

A informação electrónica custa caro, a sua utilização é principalmente profissional ou científica, deve ser rentável. Um banco de dados não está vocacionado para conter todos os conhecimentos verídicos sobre um assunto, mas o conjunto do saber utilizável por um cliente solvente. Trata-se menos de difundir esclarecimentos para um público indeterminado do que colocar uma informação operacional á disposição dos especialistas. Desta maneira, quase dois terços das informações actualmente armazenadas no mundo dizem respeito a informações económicas, comerciais ou financeiras de carácter estratégico. Os responsáveis económicos ou políticos tomam as suas decisões com base nestas informações. Os dados científicos e técnicos só vêm em segunda posição.

Em síntese, há manifesta crise pela qual perpassa o modelo contemporâneo, pois a mudança comportamental da era tecnológica que se faz presente na sociedade contemporânea é, hoje, a tônica pela qual a informática, antes matéria secundária, passa a questão primária, a exemplo de dados pessoais em relação à automação informática, que, de certo modo, antecipa as razões de prevenção, reclamando do sujeito uma ação protetiva e disposta às *consequências morais*.⁹

⁷ SENNETT, Richard. *A cultura do novo capitalismo*. Trad. Clóvis Marques. 2. ed. Rio de Janeiro: Record, 2008.

⁸ Bobbio (2004, p. 36-37) vê nisso a categorização de direitos fundamentais concorrentes à relação temporal de certa sociedade, a saber: “Cabe considerar, de resto, que as exigências que se concretizam na demanda de uma intervenção pública e de uma prestação de serviços sociais por parte do Estado só podem ser satisfeitas num determinado nível de desenvolvimento econômico e tecnológico; e que, com relação à própria teoria, são precisamente certas transformações sociais e certas inovações técnicas que fazem surgir novas exigências, imprevisíveis e inexequíveis antes que essas transformações e inovações tivessem ocorrido. Isso nos traz uma ulterior confirmação da sociabilidade, ou da não-naturalidade, desses direitos”.

⁹ A respeito da computabilidade e seu auxílio artificial Lévy (1999, p. 49) sintetiza que: “Resumindo, a extensão do ciberespaço acompanha e acelera uma virtualização geral da economia e da sociedade. Das substâncias e dos objetos,

Em face dessa situação hipotética, podem-se vislumbrar vários desdobramentos do tema da proteção de dados na era virtual, pontuando-se: a) o direito à liberdade de comunicação e autodeterminação personalíssima nas redes sociais; b) o direito à privacidade de dados pessoais, bem como da importunação do grupo em sala de aula remota; c) o direito à intimidade e suas consequências para o consentimento em participar ou não da interlocução em sítio eletrônico, bem como a manutenção da própria integridade moral nestes espaços. Com efeito, destaca-se a questão do Marco Civil da Internet em referência à Lei Geral de Proteção de Dados e potencial proteção das relações de consumo no CDC, enquanto institutos que dialogam sobre o armazenamento, disposição e proteção de dados pessoais.

2. OS PRECEITOS DA PROTEÇÃO DE DADOS NOS INSTITUTOS JURÍDICOS

Os princípios insculpidos no art. 3º da MCI e no art. 6º da LGPD, art. 4º IV e IX do CDC sustentam a normatividade e a extensão abstrata às situações pela qual o intérprete poderá fazer uso, dentre eles, os princípios da finalidade, da adequação e da necessidade dos dados, e ainda, educação e informação de fornecedores e consumidores, quanto aos seus direitos e deveres, com vistas à melhoria do mercado de consumo; fomento de ações direcionadas à educação financeira e ambiental dos consumidores.

No paradoxo do recreio das crianças em sala de aula remota, anteriormente proposto, a instituição de ensino sustentava que não era bem o diálogo moral das crianças a conferir responsabilidade à entidade escolar, pois tal liberdade de expressão é melhor regulada na Lei 12.965/2014, o Marco Civil da Internet, pois, melhor seria atribuir aos pais a esfera do consentimento e da responsabilidade por tais comportamentos virtuais, posto que os menores não demandavam o condão de fazê-lo, e à entidade escolar, havia risco para o armazenamento e tratamento de dados;¹⁰ em face disso, seria possível cotejar a perspectiva da principiologia do MCI com ao menos três princípios do art. 6º da LGPD, a saber: finalidade, adequação e necessidade.

A finalidade (art. 6º, I) a fomentar a lógica dos fatos jurídicos, isto é, quais os fins de resguardar os dados de uma pessoa e sua instrumentalidade e, uma vez utilizados com o consentimento, arregimentam o alcance de dados, levando a efeito de concretização dos fins. A adequação (art. 6º, II), diferente dos fins, ocupar-se-ia dos meios empregados para a proteção de dados, a fim de que a pessoa os consinta com razoabilidade, ao passo que a necessidade (art. 6º, III) reclamaria a natureza da utilização dos dados, posto que do contrário faz-se possível oportunizar o descarte desses mesmos dados.

voltamos aos processos que os produzem. Dos territórios, pulamos para a nascente, em direção às redes móveis que os valorizam e os desenham. Dos processos e das redes, passamos às competências e aos cenários que as determinam, mais virtuais ainda. Os suportes de inteligência coletiva do ciberespaço multiplicam e colocam em sinergia as competências. Do design à estratégia, os cenários são alimentados pelas simulações e pelos dados colocados à disposição pelo universo digital.”

¹⁰ Giddens (1991, p.160-161), em expressivo ensaio sobre as consequências sobre modernidade aprecia “[...] mesmo riscos de alta-consequência não são apenas contingências remotas, que podem ser ignoradas na vida diária, se bem que com algum provável custo psicológico. Alguns destes riscos, e muitos outros que são potencialmente ameaçadores à vida para os indivíduos ou que os afetam significativamente de outra maneira, impõem-se direto no âmago das atividades cotidianas. Isto vale, por exemplo, para qualquer dano de poluição que afete a saúde de adultos ou crianças, ou qualquer coisa que produza conteúdos tóxicos nos alimentos ou afete suas propriedades nutricionais. Isto é verdadeiro também para uma profusão de mudanças tecnológicas que influenciam as possibilidades de vida, como as tecnologias de reprodução. A mistura de risco e oportunidade é tão complexa em muitas das circunstâncias envolvidas que é extremamente difícil para os indivíduos saberem até onde atribuir confiança a prescrições ou sistemas específicos e em que medida suspendê-la.

Em breve categorização, fazendo uma reflexão do hipotético *recreio das crianças em sala virtual*, com os três princípios acima referidos, é possível entender que a instituição de ensino tem por fim respaldar-se quanto ao tratamento de dados reais e conservados em aula remota, em face de eventuais reparações judiciais, sobretudo, a responsabilidade consumerista por vício da má prestação de serviços, posto que os meios não combinariam *prima facie* com a adequação e a necessidade quanto à exclusão do espaço de recreio dos infantes, vale dizer, uma verdadeira ponderação principiológica.

De forma preventiva o CDC, por sua vez, aposta na principiologia educacional das pessoas consumidoras para que sejam melhor informadas e tenham melhor condições de decidir quanto aos seus dados pessoais, em franca autodeterminação dos sujeitos de direitos e significativo amadurecimento comportamental e nisso reside também uma plêiade de direitos básicos como os previsto no art, 6º. I, II, III do CDC.

No âmbito ainda do MCI vale destacar que sua principiologia é composta por diretrizes fundamentais que orientam a interpretação e a aplicação da lei, cuja discussão se orienta também a LGPD, pois se podem associar alguns dos elementos principiológicos expressos na LGPD à proteção de dados. Esses princípios são essenciais para garantir a proteção dos dados pessoais, por essa razão, um dos princípios do MCI, conforme o art. 3º, I, é a garantia da liberdade de expressão, comunicação e manifestação de pensamento, assegurando-se que as pessoas possam se expressar livremente na internet, respeitando a Constituição brasileira de 1988, no entanto, a aplicação prática deste princípio deve considerar o equilíbrio entre a liberdade de expressão e a necessidade de combater abusos, tais como a disseminação de discursos de ódio e desinformação.

De acordo com o art. 3º, III, o MCI promove a proteção dos dados pessoais conforme a legislação vigente e este princípio exige que os dados pessoais sejam tratados de forma transparente e responsável, garantindo que as práticas de coleta e uso estejam em conformidade com a lei. Isso é essencial para promover a confiança dos usuários e assegurar a responsabilidade das entidades que manipulam esses dados.

Vide ainda que o art. 3º, IV do MCI, destaca-se a preservação e garantia da neutralidade de rede e tal princípio assegura que todos os dados na internet sejam tratados de maneira igual, sem discriminação ou priorização, garantindo uma internet aberta e acessível, em uma palavra, a neutralidade de rede serve para manter a equidade e a liberdade na navegação online.

Na situação imaginada, os pais responsáveis só veriam descartada a segurança jurídica dos dados se o consentimento desses mesmos pais não fosse esclarecido ou consentido o suficiente para poupar a instituição de ensino de quaisquer danos à integridade moral das crianças, posto que rechaçar as crianças do ambiente virtual comum não seria suficientemente adequado em face da necessária contratação esclarecida e consentida pelos pais dos alunos e da essencialidade do bem – o livre desenvolvimento pessoal em espaço consentido por quem se faça responsável. Enfim, o recreio virtual seria a forma de convívio pelas redes sociais que, na condição de consumidores virtuais, fazem jus às crianças, cuja plataforma e segurança de dados a escola deveria assegurar.¹¹

¹¹ Sukhdev (2013, p. 186), em face do novo mundo corporativo, considera: “A internet mudou a forma pela qual as pessoas escolhem suas marcas, e forneceu uma plataforma para a troca de notícias, informações e opiniões. Ela liberou os consumidores do fardo de fazer uma escolha baseada nas promessas dos fabricantes. O impacto dessa troca de opiniões entre consumidores é mais facilmente percebido nos produtos direcionados aos jovens, o grupo demográfico que passa mais tempo na *internet* e a usa como ferramenta para a tomada de decisões. A cada 60 segundos, mais 1 200 anúncios são publicados no site Craigslist, um sinal claro de que os consumidores estão conversando entre eles.

Para tanto, só haveria violação se tais dados não levassem em consideração alguma forma negocial, com base na informação esclarecida, descortinando a negociação, de forma livre e esclarecida, quanto ao comportamento e consequências das falas de seus filhos, a disposição informada resguardaria a escola de quaisquer reparações. O art. 3º, II, estabelece a proteção da privacidade como um princípio fundamental, esse princípio exige que a coleta e o tratamento de dados pessoais sejam realizados de forma a respeitar a privacidade dos indivíduos. A proteção da privacidade é imprescindível para garantir que as informações pessoais não sejam expostas indevidamente ou usadas sem a devida autorização.

Em último caso, a escola responderia pela manutenção pífia dos dados que não são, necessariamente, da rede escolar, mas da rede tecnológica, e esse é um mundo em construção, que a inteligência artificial e o ser humano ainda não sabem controlar.¹² Para a entidade educacional, a simples interrupção da aula gravada no horário de intervalo não resolveria o problema escolar, pois, as falas e as imagens poderiam ser copiadas/reproduzidas pelos próprios usuários-alunos ou terceiros, no atual domínio tecnológico, ou seja, o espaço comunicacional é transferido para o espaço virtual, estruturado nas formas de interlocução das redes, ao que Castells (1999, p. 14-15) fomenta:

A constituição de redes é operada pelo ato da comunicação. Comunicação é o processo de compartilhar significado pela troca de informações. Para a sociedade em geral, a principal fonte da produção social de significado é o processo da comunicação socializada. Esta existe no domínio público, para além da comunicação interpessoal. A contínua transformação da tecnologia da comunicação (TI) na era digital amplia o alcance dos meios de comunicação para todos os domínios da vida social, numa rede que é simultaneamente global e local, genérica e personalizada, num padrão em constante mudança. O processo de construção de significado caracteriza-se por um grande volume de diversidade. Existe, contudo, uma característica comum a todos os processos de construção simbólica: eles dependem amplamente das mensagens e estruturas criadas, formatadas e difundidas nas redes de comunicação multimídia. Embora cada mente humana individual construa seu próprio significado interpretando em seus próprios termos as informações comunicadas, esse processamento mental é condicionado pelo ambiente da comunicação. Assim, a mudança do ambiente comunicacional afeta diretamente as normas de construção de significado e, portanto, a produção de relações de poder.

Com base no caso imaginário das crianças em sala de aula remota, podem-se associar alguns dos elementos principiológicos expressos tanto no MCI, na LGPD e no CDC quanto à proteção de dados, pois, quando os pais, responsáveis pelos menores, solicitam a reabertura do recreio virtual, a firmar a autodeterminação da liberdade de expressão e da sociabilidade dos infantes, a preocupação da direção escolar reside na maneira como esses dados estarão dispostos na plataforma digital, expondo as crianças e, ao mesmo tempo, potencialmente, criando responsabilidade ao núcleo educacional pelo tratamento e armazenamento dos dados, em tempo real ou gravados.

A velocidade na qual a informação é compartilhada entre as pessoas que pensam o mesmo modo é espantosa. Ela tornou-se um instrumento de transformação - testemunha da Primavera Árabe de 2011, movimento que demonstrou o poder da rede em facilitar a comunicação em todos os níveis e canais.”

¹² Friedman (2017, p. 241) a este respeito reflete: “Vamos deixar uma coisa clara: os robôs não estão destinados a ficar com todos os empregos. Isso só acontecerá se deixarmos – se não repensarmos toda a linha de montagem, da educação primária até a aprendizagem contínua, passando pelo trabalho.”

3. PROPOSIÇÕES DIALOGADAS DAS INSTITUIÇÕES DE PROTEÇÃO DE DADOS

No Brasil, tanto MCI, LGPD E CDC são legislações tardias para o problema antevisto, e o Código de Defesa e Proteção do Consumidor é testemunha disso, pois embora previsto na texto constitucional, art. 5º. XXXII, “na forma da lei”, fora promessa do constituinte originário no art. 48 do Ato das Disposições Constitucionais Transitórias em 120 dias, veio a ter publicação somente em 11 de setembro de 1990, a despeito ainda da sua vigência; dentre os fundamentos elencados na Lei de Dados pessoais, encontra-se o novel art. 5º. LXXIX implementado por Emenda Constitucional, a fundamentar o arcabouço de direitos fundamentais quanto à proteção de dados, mas, de logo, já era possível assegurar o *bloco de constitucionalidade*, compreendido como um conjunto de normas fundamentais, positivadas ou não, para a limitação do Estado-Sociedade Civil – sujeitos, ora como disposição de direitos humanos, ora como instrumentos regulatórios da experiência comum.

O bloco de constitucionalidade não era tábua de salvação, pois, mais necessidade de identidade constitucional e autoeducação na vida contemporânea havia do que uma série de normas a seguir, como se fossem placas indicativas de trajetos viários. Considera-se, *a priori*, o enfrentamento entre o ser humano livre e a era informacional, ou seja, a ambivalência relativa ao ente revestido de imanências libertárias, dentre elas, a liberdade de expressão, o desenvolvimento da personalidade, a dignidade humana (art. 1º., III c/c art. 5º.IV, V, IX, X; 6º. – a segurança; 7º. XXVII – a proteção em face da automação CRFB/88) e, por outro lado, a disposição cultural da sua personalidade informacional, agente que é da própria deliberação, propenso à relativização de seus dados pessoais, não raro se patrimonializando ou tornando-se objeto de consumo¹³ (art. 1º. IV c/c arts. 5º. XXI, XX, XXXII; art. 170, IV. art. 218, §§ 1º., 2º. e 3º. da CRFB/88).

Denota-se que há um sistema complexo de valores em disposição, sob as finalidades em equilíbrio entre a liberdade e a informação. A forma *ideal* é imaginar que o ser humano é auto-determinado a desenvolver-se constitucionalmente, e a forma *concreta* é conceber o ser humano vendedor de sua própria informação, de seus dados: um paradoxo evidente das dimensões humanas. Assim, em uma perspectiva complexa, vale levar a efeito outras normas constitucionais, tais como o art. 3º, IV CRFB/88, pois é imprescindível promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação.

É certo que na Constituição os direitos humanos não vigoram no psicologismo dos sujeitos, mas, por consequência, provocam a reflexão psicológica como valor fundante da integridade moral dos sujeitos, pois, se o paradoxo da vida envolve disposições e informações de direitos como a intimidade e a privacidade, falando mais alto à paz e à integridade moral das pessoas; se há predisposição constitucional para a limitação dos dados pessoais em bancos privados ou instituições públicas, é indispensável que a norma infraconstitucional acione os contornos para tais limites, para que a sociedade da informação, do consumo e da relativização de dados não venha conferir o espaço ilimitado e predatório da tecnologia sobre a dignidade humana.

Se a Constituição ainda não fala à subjetividade dos sujeitos, a reserva legal deve orientar a experiência social sobre os cuidados dos dados pessoais, que a era tecnológica não aprendeu a

¹³ Neste caso vide a reflexão de Bauman (2012, p. 12): “Os encontros dos potenciais consumidores com os potenciais objetos de consumo tendem a se tornar as principais unidades na rede peculiar de interações humanas conhecida, de maneira abreviada, como “sociedade de consumidores”. Ou melhor, o ambiente existencial que se tornou conhecido como “sociedade de consumidores” se distingue por uma reconstrução das relações humanas a partir do padrão, e à semelhança, das relações entre os consumidores e os objetos de consumo. Esse feito notável foi alcançado mediante a anexação e colonização, pelos mercados de consumo, do espaço que se estende entre os indivíduos – esse espaço em que se estabelecem as ligações que conectam os seres humanos e se erguem as cercas que os separam”.

frear, de vez que a inclinação da transgressão ao consentimento moral é comum no trato das informações em massa, vale dizer, em franca ascensão da tecnologia para fins econômicos sobre os dados das pessoas.

A cidadania de que fala o art. 5º. LXXIX do MCI e da LGPD nada mais é do que a organização social para o interesse comum, isso significa que a ética programática fala ao comportamento social, antes mesmo de interesses tecnológicos informacionais, porque a automação tecnológica não surgiu para diminuir os direitos da personalidade na era virtual, todavia, para facilitar o exercício da comunicação e a otimização íntegra dos dados pessoais.

Haverá dias em que a sistemática constitucional falará mais alto, pois, neste modelo, o sujeito constitucional não pensa em regulação do Estado à ordem tecnológica, nem espera promessas dos pactos globais, ele passa a ser protagonista dessa mesma ordem porque é um sujeito moralmente ativo, sob o risco da própria violabilidade e do interesse de seus pares, quiçá, o esclarecimento quanto à função e a finalidade tecnológica farão desse sujeito constitucional um usuário mais consciente da informação comum. Com efeito, o que se espera do MCI e da LGPD no plano da concretude dos direitos, retomando-se o complexo dos alunos em sala de aula remota?

Entender o MCI em diálogo à LGPD é transcender a simples leitura de um documento, sendo necessário compreender a normatização de um comportamento específico de um tipo social. Os dados pessoais, enquanto objeto de proteção do MCI e da LGPD, representam uma extensão dos direitos de personalidade, de sorte que a legislação ao reconhecer que os dados pessoais são uma expressão da identidade individual e, portanto, merecem proteção jurídica adequada; por certo, no contexto do MCI, LGPD e CDC, a proteção dos dados pessoais não se restringe apenas à privacidade, mas também se estende à dignidade humana e ao exercício da cidadania. Neste sentido, em ênfase à atuação consumerista a boa doutrina de Cláudia Lima Marques assinala:

É possível afirmar hoje, no Brasil, que o Supremo Tribunal Federal, os Tribunais Estaduais, o juízes de primeira instância e os JECs consolidaram o uso do método do diálogo das fontes como caminho para – em casos difíceis – assegurar a prevalência do princípio *pro homine* e desta eficácia horizontal dos direitos fundamentais por aplicação do CDC às relações privadas.¹⁴

Vale ressaltar que o art. 7º do CDC provoca o diálogo com outros ramos e fontes do direito, para tanto, os direitos previstos no Código não excluem outros decorrentes de tratados ou convenções internacionais de que o Brasil seja signatário, da legislação interna ordinária, de regulamentos expedidos pelas autoridades administrativas competentes, bem como dos que derivam dos princípios gerais do direito, analogia, costumes e equidade.

Para tanto, a doutrina do diálogo das fontes dá-se entre institutos diversos, observando-se a palavra *diálogo*, como um sistema de influências recíprocas, com respaldo na jurisprudência pátria, inclusive para o tema de controle de constitucionalidade.

Vide agora a exemplificação proposta da doutrina em torno do diálogo das fontes. No caso do *diálogo sistemático da coerência*, quando o CDC tratava da locução dados pessoais em seu art. 43, o MCI a seu turno previa a proteção de dados pessoais na *forma da lei* em seu art. 3º.

¹⁴ MARQUES, Lima Cláudia. O “diálogo das fontes” como método da nova Teoria Geral do Direito: um tributo a Erik Jayme. In: MARQUES, Cláudia Lima Marques (coord.). *Diálogo das fontes: do conflito à coordenação das normas de direito*. São Paulo: Revista dos Tribunais, 2012. p.38

III, lei que veio a dar compreensão léxica na LGPD, em seu art. 5º, I, restando à experiência da *ratio decidendi* a compreensão semântica de dados pessoais.¹⁵

Também o *diálogo sistêmico da complementariedade ou subsidiariedade*, cuja interlocução normativa é concorrente, por exemplo, a pertinência à responsabilidade civil de dados pessoais, em que a legislação reconhece que a manipulação inadequada ou abusiva dos dados pessoais pode prejudicar a dignidade humana, comprometendo seu direito à privacidade e à integridade moral; o MCI e a LGPD estabelecem medidas de segurança e transparência para garantir que os dados pessoais sejam tratados de maneira ética e responsável, respeitando os direitos fundamentais dos indivíduos, cuja normatividade do CDC vai encontrar respaldo nas responsabilidades dos fatos/vícios dos produtos e serviços.

Por essa via, princípios da LGPD, como segurança (art. 6º. VII) e responsabilidade de dados (art. 6º. X) estariam comprometidos, retomando o complexo das crianças em recreio da sala de aula rêmora, esbarrariam, como ensejavam os pais dos alunos, na principiologia da liberdade e do livre desenvolvimento da personalidade, em face do livre acesso às plataformas de dados.¹⁶

A aplicação do MCI e da LGPD alinhados com o princípio da autodeterminação informativa confere aos indivíduos o direito de decidir sobre a coleta, o uso e a divulgação de seus dados pessoais; tal principiologia reflete a ideia de que cada pessoa deve ter o controle sobre suas informações pessoais, garantindo a liberdade de escolha e a proteção contra abusos, por essa razão as instituições de proteção de dados promovem a cidadania ativa, permitindo que os indivíduos exerçam seus direitos de maneira consciente e informada.

Há ainda o *diálogo sistêmico de adaptação ou coordenação*, senão de influências recíprocas, que em último caso vai dirimir circunstâncias levadas a efeito pelos institutos, por vezes, à esteira da generalidade/especialidade, como é caso de distinguir relações de consumo de meras

¹⁵ Leia-se no seguinte Recurso inominado – Vazamento de dados pessoais de cliente por empresa fornecedora de energia elétrica – Relação de consumo – Tratamento de dados pessoais de pessoa localizada no território nacional e após 17/09/2020 – LGPD aplicável ao caso – Vazamento denota que não foram adotadas medidas de segurança eficazes pela controladora/fornecedora (art. 46 da LGPD), o que caracteriza defeito na prestação do serviço – Responsabilidade objetiva da controladora/fornecedora (art. 14 do CDC) – Ação de eventual hacker que constitui fortuito interno – Danos morais in re ipsa, conforme precedente do STJ – Indenização arbitrada em R\$ 5.000,00 – Sentença reformada – Recurso provido. (TJ-SP - RI: XXXXX20218260003 SP XXXXX-21.2021.8.26.0003, Relator: Carlos Eduardo Santos Pontes de Miranda, Data de Julgamento: 25/10/2021, 4ª Turma Recursal Cível - Santo Amaro, Data de Publicação: 25/10/2021)

¹⁶ Pensando nisso a instituição escolar reclamaria outro meio para a segurança dos dados no recreio escolar virtual, sob o risco de afastar o livre acesso de dados em situação fraqueada, questão que um jugado já entendeu viável, a reclamar a LGPD, quando um advogado egresso de uma sociedade de causídico reivindicava o acesso de dados a sua clientela profissional, senão veja-se:

“AGRAVO DE INSTRUMENTO. AÇÃO DE DISSOLUÇÃO DE SOCIEDADE. ACESSO DO EX-SÓCIO A DOCUMENTOS DA EMPRESA. FASE DE APURAÇÃO DE HAVERES. SOCIEDADE DE ADVOGADOS. LGPD. DECISÃO MANTIDA.

[...]

2. O fato do agravado não mais integrar a sociedade não lhe retira o direito de ter acesso aos contratos firmados durante sua atuação como sócio, tampouco aos documentos produzidos no mesmo período, posto que indispensáveis para a segunda fase da demanda (apuração de haveres), inclusive para eventual compensação de eventuais valores retirados a mais pelo sócio retirante. 3. **No que tange ao tratamento de dados pessoais, sob a ótica da Lei Geral de Proteção de Dados (LGPD), é indubitoso que as sociedades de advogados também devem se adaptar ao normativo. Contudo, não constar dos autos que a sociedade tenha implementado a gestão do escritório nos termos da lei, tais como elaboração de normativos internos, fluxo de dados pessoais, forma e tempo de guarda do consentimento, dentre outros, dificulta a análise de qualquer inconveniente ou ilegalidade que o acesso aos contratos possa gerar.** [grifo nosso] 4. Recurso desprovido.

(TJ-DF 07483102920208070000 DF 0748310-29.2020.8.07.0000, Relator: JOSAPHA FRANCISCO DOS SANTOS, Data de Julgamento: 22/04/2021, 5ª Turma Cível, Data de Publicação: Publicado no DJE: 04/05/2021. Pág.: Sem Página Cadastrada.)”

relações obrigacionais, típicas de tutelas específicas; vide que a teoria do diálogo das fontes foi reconhecida no Enunciado 167 da Jornada de Direito Civil, ao afirmar que, com o advento do Código Civil de 2002, houve uma forte aproximação principiológica entre este diploma e o Código de Defesa do Consumidor, especialmente na regulação contratual, dado que ambos incorporaram uma nova teoria geral dos contratos.

Na discussão deste estudo é interessante destacar que a locução *dados pessoais* nas relações da rede mundial de computadores (art. 3º. III da MCI) ou consumeristas (art. 43 do CDC) podem assumir um teor generalistas, que a Lei Geral de Proteção de Dados pode especificar, ora sob a concepção de dados pessoais sensíveis (art. 5º, II da LGPD), ora anonimizados (art. 5º, III da LGPD), ora ainda pseudonomizados (art. 12, §4º. da LGPD).¹⁷

Interessante ainda julgado emblemático, que bem se adequa a este diálogo sistêmico cuja ideia fomenta a relativização e a ponderação de dados, sob o espectro da LGPD, instrumentalizando e contracenando os princípios da transparência e da segurança jurídica, em caso paradigmático, pela qual a Corregedoria Nacional de Justiça exigia dados à instituição cartorária, ao passo que esta se recusava a fornecer *ex vi* a novel Lei de Proteção de Dados.¹⁸

¹⁷ Em face do não esclarecimento e consentimento transgredido há julgado em contrato de consumidor, cuja vítima de fraude o TJ-AP considerou os elementos da tratativa em detrimento do princípio da finalidade adequada, pela qual a LGPD fora citada uma vez que os dados do consumidor foram tratados e utilizados sem o seu devido conhecimento e consentimento - TJ-AP - RI: 00343984820198030001 AP, Relator: MÁRIO MAZUREK, Data de Julgamento: 01/04/2021, Turma recursal:

CONSUMIDOR. CONTRATO DE FINANCIAMENTO DE VEÍCULO. FRAUDE. COMPROVADA. DANOS MORAIS. COMPROVAÇÃO. VALOR DO DANO. ADEQUAÇÃO. RECURSO CONHECIDO E PROVIDO EM PARTE. SENTENÇA PARCIALMENTE REFORMADA 1) Da leitura do art. 14 do CDC, verifica-se que a responsabilidade do fornecedor de serviços é objetiva e somente não responderá pela reparação dos danos causados se provar que, tendo prestado o serviço, o defeito inexiste ou o fato é exclusivo do consumidor ou de terceiro. 2) No caso dos autos, Ficou evidente que os dados do autor, independentemente de sensíveis ou pessoais (art. 5º, I e II, Lei Geral de Proteção de Dados Pessoais - LGPD) foram tratados em violação aos fundamentos de sua proteção (art. 2º, LGPD) e à finalidade específica, explícita e informada ao seu titular (art. 6º, I, LGPD).3) Não houve contrato firmado entre as partes. Entretanto, conforme prova documental, houve a utilização de seus dados para finalidade diversa e sem que o autor tivesse informação adequada (art. 6º, II, LGPD), o que afronta diretamente o disposto no artigo 6º, III e IV, do Código de Defesa do Consumidor, quanto ao dever de informação. Assim, não existe suporte para a exclusão de responsabilidade, pois ficou caracterizado o ilícito relativo à violação de direitos da personalidade, por utilização indevida de dados pessoais. 4) Quanto aos danos morais, no caso em particular, deve ser reduzido, em consonância com os julgados desta Turma Recursal, para o valor de R\$ 4.000,00 (quatro mil reais). 5) Recurso conhecido e provido em parte. Sentença parcialmente reformada para reduzir o valor dos danos morais para R\$ 4.000,00 (quatro mil reais), permanecendo inalterados os demais termos do julgado. Sem honorários. (TJ-AP - RI: 00343984820198030001 AP, Relator: MÁRIO MAZUREK, Data de Julgamento: 01/04/2021, Turma recursal)

¹⁸ Mandado de segurança. Corregedoria Nacional de Justiça. Pedido de Providências. Provimento nº 88/2019. Posterior vigência da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais). Ausência de ato concreto a ser examinado na perspectiva da suposta violação de direito líquido e certo. Impetração voltada ao exame de ato normativo em tese. Súmula nº 266/STF. Não conhecimento da impetração. Inicial indeferida (art. 10 da Lei nº 12016/09). Vistos etc.

[...]

2. Sustentam que, na qualidade de delegatárias de serviços extrajudiciais, são controladoras de dados pessoais (art. 5º, VI, da Lei Geral de Proteção de Dados Pessoais – LGPD, em conjunto com o item 129 do Capítulo XIII do Tomo II das Normas de Serviço da Corregedoria Geral da Justiça do Estado de São Paulo), sendo por estes responsáveis. Contudo, o Provimento nº 88 da Corregedoria Nacional de Justiça (publicado em 1º.10.2019) as obrigaria ao compartilhamento dessas informações em hipóteses reputadas desconformes aos limites estabelecidos pela LGPD (Lei nº 13.709/2018).

[...]

As próprias alegações ressaltam a tentativa de fazer valer o mandado de segurança como ação de impugnação de ato normativo em abstrato, à consideração da contagem do prazo decadencial a partir da entrada em vigor da LGPD, esta contrastada, em sua essência, ao anterior Provimento nº 88, com o objetivo de retirar, deste, a compatibilidade com o ordenamento.

A tecnologia se traduz no espaço da alta modernidade como um mensageiro para a transformação desse cenário, com isso a reflexão comportamental não é só uso da legislação a regular a experiência comum, se, a exemplo da Lei Geral de Proteção de Dados, a esfera regulatória se faz, insuficientemente, incapaz de acompanhar a célere difusão e impropriedade dos dados, mercadejando-se a personalidade das pessoas pelas redes, é, antes, um apelo para o mundo que se constrói sem limites e destacado pela inconsequência moral dos grandes dados de massa.

As leis contemporâneas das tecnologias têm o mérito de exprimir a disposição das liberdades em um cenário complexo, mas, a par disso, o esforço regulatório deve sair da esfera pública para entronizar-se na sociedade civil, na cidadania privatista das pessoas a erradicar a pessoa-produto em uma civilização para o consumo.

Por essa razão, as soluções contemporâneas recaem sempre sobre soluções contingenciais ou convencionais que não dispõem de ferramentas eficientes para o desiderato das redes virtuais. Porém, se as leis da era tecnológica não respeitam os direitos da personalidade, é melhor retomar o velho caminho humano, em que o homem é a medida de todas as coisas, conduzida pelo antropocentrismo universal e não o tecnocentrismo, a domar os direitos de personalidade das pessoas.

Por fim, é importante destacar que a proteção dos dados pessoais e a garantia dos direitos de personalidade são essenciais para a construção de uma sociedade justa e democrática, onde o MCI e LGPD, ao proteger os dados pessoais, contribuem para a promoção dos direitos humanos, garantindo que os indivíduos sejam tratados com dignidade, respeito e igualdade, por certo, a legislação estabelece um equilíbrio entre o avanço tecnológico e a proteção dos direitos fundamentais, assegurando que a evolução da sociedade digital ocorra de maneira ética e responsável.

CONSIDERAÇÕES FINAIS

A inclusão digital no mundo fez prematura uma plêiade de legislações sob à égide do Terceiro Milênio, sob outro prisma, são legislações tardias dada a celeridade que o mundo coloca as invenções tecnológicas, daí a preocupação sistemática do ordenamento jurídico, e por consequências da forma dialogada pela qual devem tecer as instituições jurídicas; por essa razão, as dobras do diálogo das fontes, o Marco Civil da Internet, a Lei Geral de Proteção de Dados e o Código de Defesa do Consumidor se entrelaçam com a roupagem que lhes foram oportunamente oferecidas, daí as atualizações legislativas dos diplomas, e mesmo de eventual controle de constitucionalidade a que se submetem essas normas.

Enquanto a aparência de um arcabouço sólido se projeta, a realidade da era tecnológica denuncia lacunas que deixam as pessoas expostas em sua vulnerabilidade digital e a promessa de proteção esbarra na insuficiência de práticas efetivas, numa dança entre regulação e transformação que clama por maior profundidade crítica, e ao refletir sobre a complexidade do cenário, emerge a questão: até onde se está disposto a avançar para garantir a autodeterminação das pessoas frente à tecnologia? A resposta, ainda distante, perpassa não apenas a aplicação das normas existentes, mas a reinvenção do papel do direito em um ambiente de constante inovação.

(STF - MS: 37636 DF 0036489-15.2021.1.00.0000, Relator: ROSA WEBER, Data de Julgamento: 19/01/2021, Data de Publicação: 22/01/2021)

Nesse processo, o diálogo das fontes desponta como um farol, iluminando a necessidade de articulação entre legislações que, embora distintas, convergem na proteção da dignidade humana em um mundo cada vez mais mediado por algoritmos, não obstante, a proteção que tais legislações oferecem requer uma integração que vá ao encontro das experiências humanas.

Neste sentido, o futuro das legislações voltadas à proteção de dados e direitos no ambiente digital não pode ser apenas técnico, mas profundamente humano, alicerçado em princípios que coloquem as pessoas, sua privacidade e dignidade, no centro das transformações e os desafios relacionados aos direitos em meio às culturas cibernéticas não se limitam a frear o desenvolvimento das redes ou das tecnologias inteligentes, todavia, envolvem a criação de instrumentos regulatórios transnacionais, em uma era de interconexão global.

No cenário hipotético do recreio virtual em salas de aula remotas, emerge uma intrincada teia de relações entre liberdade de expressão, responsabilidade pelo tratamento de dados e autodeterminação informativa dos consumidores, de tal modo que abordagem principiológica subjacente aos dispositivos normativos examinados não apenas oferece diretrizes interpretativas, mas também propõe um equilíbrio dinâmico entre os interesses de proteção individual e as exigências estruturais de uma sociedade conectada.

No contexto do recreio virtual, a aplicabilidade dos princípios da finalidade, adequação e necessidade, previstos na LGPD, e dos direitos básicos do consumidor, assegurados pelo CDC, demonstra como a normatividade orienta o comportamento das partes envolvidas. A escola, como fornecedora de serviços, carrega o ônus de assegurar um ambiente digital seguro e funcional, sem negligenciar o direito à sociabilidade das crianças. Por outro lado, os pais devem ser informados de maneira clara e acessível, de modo a exercerem o consentimento de forma consciente e esclarecida.

O desafio de balancear o avanço tecnológico com a garantia de direitos exige um esforço coletivo e contínuo de reflexão, regulação e educação, a fim de construir uma sociedade que compreenda e respeite o valor dos dados pessoais no contexto contemporâneo, ao passo que a contemporaneidade revela-se um palco de paradoxos, pois entre o avanço das tecnologias e os direitos de personalidade, vive-se o embate constante entre a autonomia do indivíduo e a mercantilização de sua identidade informacional. O Marco Civil da Internet (MCI), a Lei Geral de Proteção de Dados (LGPD) e o Código de Defesa do Consumidor (CDC), ao mesmo tempo que se consolidam como marcos regulatórios indispensáveis, denunciam, pela sua própria existência tardia, a insuficiência histórica do aparato normativo para acompanhar a dinâmica da sociedade informacional.

Essas legislações, contudo, são mais que um esforço legislativo; são uma tentativa de resgatar o humano no ambiente digital, impondo freios ao tecnocentrismo e revalorizando a centralidade da dignidade humana. Não basta regular o uso de dados pessoais como se fossem apenas bens econômicos: é preciso ressignificar seu lugar no mosaico das liberdades, da cidadania e da personalidade, permitindo que o sujeito digital seja protagonista de sua própria história informacional, e não mero produto do mercado de dados.

Nesse cenário, o diálogo das fontes jurídicas emerge como um instrumento poderoso para a concretização dos direitos fundamentais em um ambiente normativo complexo. A interseção entre o MCI, a LGPD e o CDC exemplifica como normas diversas podem atuar em complementaridade, garantindo um equilíbrio entre liberdade e segurança, entre inovação tecnológica e preservação da dignidade. Porém, como bem pontuado, o verdadeiro desafio não reside apenas na criação de normas, mas na capacidade de transpor os limites da regulação estatal para a autoeducação da sociedade civil, onde cada indivíduo compreenda a importância de sua atuação consciente e ética no espaço digital.

REFERÊNCIAS

- BAUMAN, Zygmunt. *Vida para consumo: a transformação das pessoas em mercadoria*. Trad. Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2012.
- BOBBIO, Norberto. **A era dos direitos**. 7. reimp. Trad. Carlos Nelson Coutinho. Rio de Janeiro: Elsevier, 2004.
- BONAVIDES, Paulo. **Curso de Direito Constitucional**. 32. ed. São Paulo: Malheiros, 2017.
- BRASIL. Constituição da República Federativa do Brasil de 1988. **planalto**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 20 fev. de 2021.
- BRASIL. Lei Geral de Proteção de Dados. **planalto**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em 20 fev. de 2024.
- BRASIL. Marco Civil da Internet. **planalto**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm. Acesso em 18 out. de 2024.
- BRASIL. Código de Proteção e Defesa do Consumidor. **planalto**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em 15 abr. de 2024.
- CANTALI, Fernanda Borghetii. **Direitos da personalidade: disponibilidade relativa, autonomia privada e dignidade humana**. Porto Alegre: Livraria do Advogado, 2009.
- CASTELLS, Manuel. **A sociedade em rede**. Trad. Roneide Venâncio 6a.ed. São Paulo: Paz e Terra, 1999. (A era da informação: economia, sociedade e cultural; v.1).
- FRIEDMAN, Thomas L. **Obrigado pelo atraso: um guia otimista para sobreviver em um mundo cada vez mais veloz**. Trad. Cláudio Figueiredo. Rio de Janeiro: Objetiva, 2017.
- GIDDENS, Anthony. **As consequências da modernidade**. Trad. Raul Fiker. São Paulo: UNESP, 1991. (Biblioteca básica).
- LÉVY, Pierre. **A esfera semântica**. Tomo I: computação, cognição e economia da informação. São Paulo: Annablume, 2014. (Coleção Atopos).
- LÉVY, Pierre. **Cibercultura**. Trad. Carlos Irineu da Costa. São Paulo: Ed. 34, 1999. (Coleção Trans).
- MARQUES, Lima Cláudia. O “diálogo das fontes” como método da nova Teoria Geral do Direito: um tributo a Erik Jayme. In: MARQUES, Cláudia Lima Marques (coord.). **Diálogo das fontes: do conflito à coordenação das normas de direito**. São Paulo: Revista dos Tribunais, 2012. pp.17-43.
- TJ-AP - RI: **00343984820198030001 AP**, Relator: MÁRIO MAZUREK, Data de Julgamento: 01/04/2021, Turma recursal.
- TJ-DF **07483102920208070000 DF 0748310-29.2020.8.07.0000**, Relator: JOSAPHA FRANCISCO DOS SANTOS, Data de Julgamento: 22/04/2021, 5ª Turma Cível, Data de Publicação: Publicado no DJE: 04/05/2021. Pág.: Sem Página Cadastrada.)”
- SEN, Amartya, KLIKSBERG, Bernardo. **As pessoas em primeiro lugar: a ética do desenvolvimento e os problemas do mundo globalizado**. Trad. Bernardo Ajzenberg, Carlos Eduardo Lins da Silva. São Paulo: Companhia das Letras, 2010.

SENNETT, Richard. **A cultura do novo capitalismo**. Trad. Clóvis Marques. 2. ed. Rio de Janeiro: Record, 2008.

SOUZA, Rogério da Silva e; ROCHA, Maria Vital da. Os direitos de personalidade na era tecnológica em especial à lei geral de proteção de dados. In: Etiene Luiza Ferreira Pleti; Heloisa Helena de Almeida Portugal; Jefferson Patrik Germinari. (Org.). **Direito Digital e Desenvolvimento**: olhares transdisciplinares sobre a efetivação de direitos. 1a.ed.Uberlândia: LAECC, 2022, v. , p. 231-246.

SUKHDEV, Pavan. **Corporação 2020**: como transforma as empresas para o mundo de amanhã. Trad. Isabel Muray. São Paulo: Abril, 2013.

STF - **MS: 37636 DF 0036489-15.2021.1.00.0000**, Relator: ROSA WEBER, Data de Julgamento: 19/01/2021, Data de Publicação: 22/01/2021.

MARCO CIVIL JUDICIAL DA INTERNET: PROMOVENDO DIREITOS E RESPONSABILIZAÇÃO NA NOVA ORDEM ECONÔMICA DIGITAL

André de Carvalho Ramos

Centro Universitário Alves Faria (UNIALFA), Goiás.
andre.ramos@unialfa.com.br

Ricardo Luiz Nicoli

Centro Universitário Alves Faria (UNIALFA), Goiás.
ricardo.nicoli@unialfa.com.br

Resumo: No contexto da evolução da regulação da internet no Brasil, destacando-se a importância do Marco Civil da Internet (Lei nº 12.965/2014) na proteção de direitos fundamentais e na responsabilização dos provedores de aplicações, o problema da pesquisa discute a adaptação da legislação às novas demandas da economia digital e garantir a efetividade das decisões judiciais diante da ubiquidade da internet. O objetivo geral consiste em investigar como o Marco Civil da Internet foi densificado por decisões judiciais paradigmáticas, promovendo a responsabilização dos provedores e superando barreiras à soberania econômica estatal. A metodologia adotada envolve a análise de casos paradigmáticos do Supremo Tribunal Federal (STF) e do Superior Tribunal de Justiça (STJ) sobre a responsabilização dos provedores de aplicações de internet e o alcance das decisões judiciais brasileiras. Discutem-se os princípios, garantias, direitos e deveres estabelecidos pela lei, incluindo a proteção da privacidade, a neutralidade da rede e a responsabilidade dos provedores; analisa-se a decisão do STF sobre a imposição de sanções econômicas a empresas que descumpram ordens judiciais brasileiras, reforçando a soberania digital; examina-se a decisão do STJ sobre a indisponibilidade global de conteúdo difamatório, destacando a jurisdição civil brasileira sobre conteúdos ilícitos na internet; e aborda-se o julgamento do STF sobre a constitucionalidade do artigo 19 do Marco Civil da Internet e a responsabilidade das plataformas digitais pelo conteúdo publicado por terceiros. Conclui-se que as decisões judiciais analisadas fortalecem a proteção de direitos fundamentais e a responsabilidade das plataformas digitais, alinhando-se a tendências internacionais de regulação da economia digital. **Palavras chave:** Marco Civil da Internet. Responsabilidade civil. Provedores de aplicação. Economia digital. Poder Judiciário.

Brazilian Judicial Civil Rights Framework for the Internet: promoting rights and accountability in the new digital economic order

Abstract: In the context of the evolution of internet regulation in Brazil, highlighting the importance of the Brazilian Civil Framework for the Internet (Law No. 12,965/2014) in the protection of fundamental rights and the liability of application providers, the research problem discusses the adaptation of legislation to the new demands of the digital economy and ensuring the effectiveness of judicial decisions in the face of the ubiquity of the internet. The general objective is to investigate how the Brazilian Civil Framework for the Internet has been intensified by paradigmatic judicial decisions, promoting the accountability of providers and overcoming barriers to state economic sovereignty. The methodology involves the analysis of paradigmatic cases from the Brazilian Supreme Federal Court (STF) and Superior Court of Justice (STJ) regarding the accountability of internet application providers and the reach of Brazilian judicial decisions.

The principles, guarantees, rights, and duties established by the law are discussed, including the protection of privacy, network neutrality, and provider responsibility; the STF's decision on the imposition of economic sanctions on companies that fail to comply with Brazilian judicial orders, reinforcing digital sovereignty, is analyzed; the STJ's decision on the global unavailability of defamatory content, highlighting Brazilian civil jurisdiction over illicit internet content, is examined; and the STF's judgment on the constitutionality of Article 19 of the Brazilian Civil Framework for the Internet and the responsibility of digital platforms for content published by third parties is addressed. It is concluded that the analyzed judicial decisions strengthen the protection of fundamental rights and the accountability of digital platforms, aligning with international trends in digital economy regulation.

Keywords: Brazilian Civil Framework for the Internet. Civil liability. Application providers. Digital economy. Judiciary branch.

INTRODUÇÃO: O MARCO CIVIL JUDICIAL DA INTERNET

O avanço da economia digital e a crescente importância das plataformas na circulação de informações e dados (com repercussões econômicas) resultaram em novos desafios regulatórios, especialmente no que se refere à previsão de responsabilização civil dos provedores de aplicações na internet por danos causados por conteúdos publicados por terceiros, bem como sobre o alcance das decisões judiciais diante da deslocalização territorial da internet.

A proposta do presente artigo é investigar de que modo o Marco Civil da Internet (Lei nº 12.965/2014) foi densificado, nesses 10 anos, por decisões judiciais paradigmáticas que buscam responsabilizar os provedores de aplicações na internet, ao mesmo tempo em que superam eventuais barreiras à soberania econômica estatal advindas da ubiquidade da internet, cuja configuração técnica ultrapassa as fronteiras políticas dos Estados.

Para tanto, foram escolhidos casos paradigmáticos do Supremo Tribunal Federal e do Superior Tribunal de Justiça sobre a responsabilização dos provedores de aplicações de internet e o alcance das decisões judiciais brasileiras. Esses dois pontos se entrelaçam: eventual opção soberana brasileira por responsabilizar os provedores (inclusive exigindo a retirada de conteúdo ilícito) seria comprometida e teria quase nenhuma efetividade se a ordem judicial fosse adstrita aos sites brasileiros ou aos locais de armazenamento de dados situados no Brasil.

O presente artigo é dividido em quatro partes. Inicialmente, foram analisados os principais aspectos do Marco Civil da Internet, que serão, após, densificados nos casos paradigmáticos.

A segunda parte do presente artigo aborda a atuação do Judiciário brasileiro na regulação digital com efeitos extraterritoriais, a qual foi objeto de análise no Recurso Especial nº 2147711 - SP (2024/0065404-7), julgado pelo Superior Tribunal de Justiça (STJ), no qual se discutiu a possibilidade de uma ordem judicial brasileira determinar a indisponibilidade global de conteúdo considerado ilícito. Esse precedente interpreta o art. 5º do Marco Civil da Internet e cria importante reforço da soberania digital brasileira, que exige das empresas transnacionais da era digital que aqui operam que cumpram as ordens judiciais brasileiras em todo o globo.

A terceira parte do artigo aborda a Ação Direta de Constitucionalidade n. 51, que trata também da jurisdição internacional cível brasileira com alcance extraterritorial, dispensando-se o uso de tratados de cooperação jurídica internacional. Tal precedente problematiza o alcance do art. 11 do Marco Civil da Internet, em novo reforço da soberania digital brasileira.

Finalmente, a quarta parte diz respeito à responsabilização cível dos provedores de aplicações da internet. Esse debate está atualmente em curso (na data de fechamento deste artigo) no

Supremo Tribunal Federal no julgamento do Recurso Extraordinário (RE) nº 1.037.396, que discute a constitucionalidade do artigo 19 do Marco Civil da Internet (Lei nº 12.965/2014). Tal dispositivo estabelece que os provedores de aplicações de internet somente podem ser responsabilizados civilmente pelo conteúdo gerado por terceiros se houver descumprimento injustificado de ordem judicial específica determinando a remoção do material questionado.

A controvérsia analisada no julgamento do RE nº 1.037.396 levanta uma dúvida central para a economia digital: a responsabilização dos provedores de conteúdo por danos causados pelos usuários restringiria desproporcionalmente a autonomia privada e o modelo de negócios das plataformas digitais, ofendendo a livre-iniciativa e trazendo novos custos de difícil previsão?

Esses três precedentes (um deles ainda em trâmite) cumprem a proposta do artigo, que é investigar o modo pelo qual o Poder Judiciário brasileiro (re)configurou o Marco Civil da Internet a favor do cumprimento de ordens judiciais brasileiras com claro impacto na nova ordem econômica digital, responsabilizando as plataformas digitais globais (os grandes provedores de aplicações de internet, incluindo os provedores de busca) e ainda reforçando o direito de terceiros à reparação de danos.

1 ASPECTOS GERAIS DO MARCO CIVIL DA INTERNET

A regulação da internet para fins civis no Brasil é disciplinada pelo Marco Civil da Internet (Lei nº 12.965/2014), que estabelece princípios, garantias, direitos e deveres para o uso da rede no país. Conforme Eduardo Tomasevicius Filho, a proposta de regulamentação foi concebida inicialmente em 2009 em parceria do Ministério da Justiça com a Escola de Direito do Rio de Janeiro, da Fundação Getúlio Vargas (FGV Direito Rio, 2014), o que resultou na apresentação de um projeto de lei ao Congresso Nacional, registrado sob o n. 2.126/2011, convertido na Lei n.12.965, de 23 de abril de 2014¹. O citado autor ressalta ainda o efeito – na época – da eclosão, em 2013, do escândalo de espionagem de escala global realizado pelo governo dos Estados Unidos, tendo sido revelada a interceptação e análise de dados transmitidos pela internet, além de práticas de espionagem contra chefes de Estados e empresas de grande porte, com o intuito de obtenção de vantagens comerciais².

Como revelam Carlos Affonso Souza e Ronaldo Lemos, as revelações feitas por Edward Snowden sobre o desenvolvimento de programas estatais norte-americanos de espionagem, e em especial voltados para o governo brasileiro consolidaram o Marco Civil como “parte da resposta nacional aos escândalos envolvendo o aumento indiscriminado de vigilância e espionagem”³. Esse foi o ambiente no qual foi adotado o Marco Civil.

A normatividade legislativa reconhece a necessidade de um marco regulatório específico para a internet, considerando sua importância para a comunicação, a economia digital e a proteção dos direitos fundamentais dos usuários.

Seu artigo 1º estabelece que suas disposições regulam o uso da internet no Brasil e orientam a atuação da União, dos Estados, do Distrito Federal e dos Municípios na matéria. O artigo 5º, por sua vez, define a internet como um sistema estruturado em escala mundial, fundamentado

¹ TOMASEVICIUS FILHO, Eduardo. Marco Civil da Internet: uma lei sem conteúdo normativo. **Estudos Avançados**, v. 30, p. 269-285, 2016, em especial p. 273.

² TOMASEVICIUS FILHO, Eduardo. Marco Civil da Internet: uma lei sem conteúdo normativo. **Estudos Avançados**, v. 30, p. 269-285, 2016, em especial p. 272.

³ SOUZA, Carlos Affonso; LEMOS, Ronaldo. **Marco civil da internet: construção e aplicação**. Juiz de Fora: Editar, 2016, p. 25.

em protocolos lógicos que possibilitam a comunicação entre redes e dispositivos, o que reforça a complexidade de sua regulação nacional (como veremos, o Poder Judiciário brasileiro utilizará esse reconhecimento legal do alcance global da internet para dar efetividade mundial às decisões brasileiras) e a necessidade de diretrizes claras para o funcionamento e a responsabilidade dos agentes envolvidos.

O artigo 2º elenca os fundamentos da regulação da internet no Brasil, incluindo o respeito à liberdade de expressão, a proteção dos direitos humanos, a preservação da diversidade e da pluralidade, a livre iniciativa e concorrência e a finalidade social da rede. Esses princípios orientam a interpretação e aplicação do Marco Civil da Internet, garantindo que a regulação da rede leve em consideração tanto os avanços tecnológicos quanto a necessidade de proteção de direitos fundamentais, incluindo a autonomia e a livre-iniciativa.

O artigo 3º complementa essa estrutura ao estabelecer princípios específicos, como a proteção da privacidade e dos dados pessoais, a neutralidade da rede, a segurança e estabilidade da infraestrutura digital, a responsabilização proporcional dos agentes da internet e a manutenção do caráter participativo e descentralizado da rede.

A legislação também define objetivos para a regulação da internet. O artigo 4º estabelece que a disciplina do uso da rede deve promover o acesso universal à internet, garantindo a inclusão digital e permitindo que a rede seja um instrumento de disseminação de informação, conhecimento e participação cidadã. Além disso, o dispositivo prevê o estímulo à inovação tecnológica, incentivando o desenvolvimento de novos modelos de uso e a adoção de padrões abertos para garantir interoperabilidade e acessibilidade.

No que se refere à responsabilidade civil, há importante diferenciação entre os provedores de serviços de acesso à internet, que são tidos como intermediários (viabilizando tecnicamente a conexão com a rede mundial de computadores) e, por consequência, não são responsáveis pelo conteúdo gerado por terceiros, conforme a literalidade do art. 18 (“Art. 18. O provedor de conexão à internet não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros”).

Por outro lado, os provedores de aplicações da internet (que gerenciam e lucram com conteúdos de terceiros) são responsabilizados de acordo com o artigo 19, o qual estabelece que tais empresas somente poderão ser responsabilizadas civilmente por danos decorrentes de conteúdos gerados por terceiros se, (i) após ordem judicial específica, (ii) não adotarem as providências necessárias para a indisponibilização do material apontado como ilícito.

Essa regra visa assegurar a liberdade de expressão e impedir censura privada, garantindo que a remoção de conteúdos na internet seja precedida de um controle jurisdicional. O parágrafo 1º do dispositivo determina que a ordem judicial deve conter identificação clara e específica do conteúdo infrator, permitindo sua localização inequívoca e evitando remoções genéricas ou desproporcionais.

O artigo 21 traz uma exceção à exigência de ordem judicial prévia para remoção de conteúdo. Ele prevê que os provedores de aplicações na internet são responsáveis subsidiariamente pela divulgação não autorizada de imagens, vídeos ou materiais contendo nudez ou atos sexuais de caráter privado. Nesses casos, a remoção não depende de decisão judicial, bastando que a vítima ou seu representante legal notifique a plataforma para que esta atue de forma diligente e indisponibilize o conteúdo.

Essa preponderância da liberdade de expressão já atraiu críticas no momento das discussões sobre o projeto de lei que redundou no Marco Civil. Marcelo Thompson defendeu que o

Marco Civil, ao veladamente separar direitos humanos em grupos distintos, na prática neutralizou direitos como honra e vida privada (que dependem de ações judiciais), criando “demarcações irrazoáveis e incompatíveis com as possibilidades democráticas do mundo contemporâneo”⁴.

Por sua vez, nada impede que as próprias plataformas tenham suas regras de moderação e de conteúdo proibido. Essa combinação (liberdade para moderar e excluir ao talante da autonomia privada e ordem judicial para quase todos os demais conteúdos) permitiu modelos de negócios que monetizavam conteúdo ilícito (pela alavanca do engajamento digital), desequilibrando a proteção de direitos. A exigência de ordem judicial como etapa indispensável para uma posterior responsabilização dos provedores de aplicações e conteúdo da internet (inclusive os buscadores) estimulou, nesses dez anos, a permissividade com *fake news*, discursos de ódio e outras manifestações que, por gerarem engajamento e forte monetização, não eram espontaneamente retiradas pelas empresas digitais.

Como destaca Cíntia Lima, antes da promulgação do Marco Civil da Internet, o entendimento predominante era de que a mera ciência do conteúdo ilícito, ainda que informada diretamente pela vítima, já seria suficiente para fundamentar a responsabilização dos provedores.⁵ Com a redação do art. 19, os provedores de conteúdo lograram importante vitória legislativa, exigindo-se o uso prévio (e mais dificultoso) do Poder Judiciário, como visto acima.

Chiara Spadaccini de Tefé e Maria Celina Bodin de Moraes entendem que o Marco Civil da Internet criou instrumentos insuficientes à tutela da pessoa na internet. As autoras destacaram “o modelo de negócio e o alto ganho financeiro” desses provedores privados de aplicações da internet, não se podendo admitir uma completa imunidade.⁶

Há, assim, uma dimensão econômica não prevista na redação aparentemente racional do artigo 19 do Marco Civil da Internet. Ao longo dos anos, ficou evidente que a racionalidade econômica capitalista havia gerado uma proteção a comportamentos empresariais de exploração lucrativa dos mais diversos conteúdos ilícitos na internet.

Ao mesmo tempo, não havia nenhuma vedação à exclusão de conteúdo por violação de termos de uso ou políticas empresariais dos mesmos provedores. O combate à “censura privada” por intermédio da exigência de ordem judicial para a retirada de conteúdo ilícito era unilateral e não abrangia o próprio provedor, que continuou – em nome da autonomia privada e livre-iniciativa – a poder retirar conteúdo considerado ilícito ou irregular. Caso houvesse abuso, o prejudicado é que teria que recorrer ao Poder Judiciário.

Para Patrícia Heloisa de Carvalho, o Marco Civil da Internet ocasionou “verdadeiro retrocesso” na proteção dos direitos fundamentais, uma vez que a redação do artigo 19 “peca por restringir deliberadamente a essência de outros direitos fundamentais, quais sejam, à privacidade, intimidade e proteção ao consumidor, fazendo com que haja verdadeiro retrocesso às garantias aos direitos humanos que já foram conquistadas até aqui”.⁷

⁴ THOMPSON, Marcelo. Marco Civil ou Demarcação de Direitos? Democracia, Razoabilidade e as Fendas na Internet do Brasil. *Revista de Direito Administrativo*, v. 261, p. 203-251, 2012, em especial p. 214.

⁵ LIMA, Cíntia Rosa Pereira de. A responsabilidade civil dos provedores de aplicação de internet por conteúdo gerado por terceiro antes e depois do Marco Civil da Internet (Lei n. 12.965/14). *Revista da Faculdade de Direito, Universidade de São Paulo*, v. 110, p. 155-176, 2015.

⁶ TEFÉ, Chiara Spadaccini de; MORAES, Maria Celina Bodin de. Redes sociais virtuais: privacidade e responsabilidade civil. Análise a partir do Marco Civil da Internet. *Pensar*, Fortaleza, v. 22, n. 1, p. 108-146, jan./abr. 2017, em especial p. 142.

⁷ CARVALHO, Patrícia Heloisa de. O “Marco Civil da Internet”: uma análise sobre a constitucionalidade do artigo 19. *Revista da Faculdade de Direito do Sul de Minas*, v. 33, n.2 p. 228-244, 2017, em especial p. 217.

Por isso, houve reação do Poder Judiciário, em caso paradigmático ainda em trâmite, que pode resultar na declaração de inconstitucionalidade do artigo 19, como veremos na quarta parte deste artigo.

Também em aspecto estudado nos precedentes judiciais abaixo, o artigo 11⁸ determina que qualquer operação de coleta, armazenamento, guarda e tratamento de registros, dados pessoais ou comunicações realizadas por provedores de conexão e de aplicações de internet, quando pelo menos um desses atos ocorrer em território nacional, deve obrigatoriamente respeitar a legislação brasileira, assegurando a privacidade, a proteção de dados e o sigilo das comunicações.

Essa obrigação se aplica independentemente do local onde os dados estejam armazenados ou da sede da empresa responsável pelo serviço, desde que haja vínculo com o Brasil. Além disso, o dispositivo prevê que os provedores devem prestar informações que permitam verificar o cumprimento da legislação, garantindo maior transparência na governança dos dados digitais. Este artigo 11 foi debatido exaustivamente no primeiro precedente estudado, que vem a ser o caso da Ação Direta de Constitucionalidade n. 51.

2 A ADC N. 51 E ARTIGO 11 DO MARCO CIVIL DA INTERNET: O USO DE SANÇÕES ECONÔMICAS DE COERÇÃO E O ACESSO AO MERCADO DIGITAL BRASILEIRO

Em 2017, foi interposta, perante o Supremo Tribunal Federal, a Ação Direta de Constitucionalidade (ADC) n. 51, que buscava a declaração de constitucionalidade do Decreto n. 3.810/2001, que promulgou internamente o “Acordo de Assistência Judiciária em Matéria Penal entre o Governo da República Federativa do Brasil e o Governo dos Estados Unidos da América”.

A controvérsia girava em torno da interpretação do artigo 11 do Marco Civil da Internet (Lei nº 12.965/2014), que exige das empresas de tecnologia a obediência à legislação brasileira sempre que os dados em questão possuem vínculo com o Brasil. A dúvida central era se seria constitucional a imposição de sanções a empresas prestadoras de serviços de conteúdo na internet (ou mesmo aos seus dirigentes) que descumprissem ordens judiciais brasileiras baseadas no Marco Civil da Internet, quando tais ordens determinassem o fornecimento de dados vinculados ao Brasil, mas armazenados no exterior – especificamente nos Estados Unidos, por decisão empresarial.

As empresas alegavam que as autoridades brasileiras deveriam necessariamente recorrer ao Acordo de Assistência Judiciária em Matéria Penal firmado com os Estados Unidos, sob o argumento de que os dados estavam armazenados naquele país e, portanto, submetidos à legislação local. Segundo essa tese, como o Marco Civil da Internet não impôs a obrigação de armazenamento local de dados (opção do legislador brasileiro), o Brasil deveria requerer tais informações às autoridades norte-americanas e se sujeitar às regras de proteção à privacidade e liberdade de expressão dos Estados Unidos. Caso o governo norte-americano, com base na sua própria interpretação desses direitos, recusasse a cooperação ou simplesmente não respondesse ao pedido, o Brasil não poderia adotar medidas coercitivas diretas. A única alternativa, segundo

⁸ Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.

essa lógica, seria denunciar o tratado e modificar a legislação para exigir o armazenamento local de dados, assegurando o cumprimento das ordens judiciais brasileiras.

No julgamento da ADC 51, o STF analisou, de forma mais ampla, a constitucionalidade do art. 11 do Marco Civil da Internet e do art. 18 da Convenção de Budapeste sobre Crime Cibernético (2001⁹).

No julgamento (ADC 51, voto do Min. Relator Gilmar Mendes, j. 23-2-2023), o STF decidiu que as hipóteses de requisição direta pelo Judiciário brasileiro, previstas no art. 11 do Marco Civil da Internet e no art. 18 da Convenção de Budapeste, fundamentam-se nos princípios da soberania e da independência nacional, concretizando o dever do Estado de proteger os direitos fundamentais, bem como o direito à segurança pública dos brasileiros e residentes no país (art. 144 da CF/88). Assim, o princípio da especialidade do Marco Civil da Internet afasta a aplicação automática da cooperação jurídica internacional nesses casos. Para o STF, a jurisdição internacional brasileira não deve ser delimitada somente com base no uso do princípio da territorialidade.¹⁰

Além dele, devem ser considerados os critérios do controle sobre os dados e dos efeitos da atividade. Pelo critério dos efeitos, a jurisdição do Estado onde ocorreu a coleta de dados e a oferta dos serviços de comunicação é legítima perante o direito internacional, ainda que a operação não tenha sido exclusivamente local.

Assim, para o STF, a jurisdição internacional brasileira não pode depender da vontade de outro Estado para a prática de atos que tenham vínculo com o território nacional. Isso decorre do princípio da autodeterminação dos povos e da igualdade entre os Estados, não podendo a soberania brasileira ser condicionada à resposta – ou ausência dela – de outro país. Contudo, quando não houver vínculo direto com o Brasil, a obtenção de dados armazenados no exterior dependerá da cooperação jurídica internacional.¹¹

Por essa razão, o STF determinou que empresas de serviços digitais devem cumprir as ordens judiciais brasileiras sempre que houver jurisdição do Brasil, independentemente da localização dos dados.

No entanto, como o Brasil não possui jurisdição de execução sobre Estados estrangeiros, o cumprimento das decisões judiciais pode depender de medidas indiretas. Isso inclui sanções econômicas e outras medidas coercitivas sobre as pessoas jurídicas do grupo econômico que operam no Brasil, a fim de garantir a efetivação das ordens judiciais. Esse mecanismo busca impedir que grandes conglomerados empresariais utilizem estruturas corporativas para se evadir à responsabilização, conforme previsto no art. 11 do Marco Civil da Internet. Na economia digital, tais sanções indiretas de coerção econômica podem inclusive conter a suspensão do serviço desses provedores de aplicações ou de conteúdo da internet.

⁹ A Convenção de Budapeste já foi ratificada e incorporada internamente pelo Dec. n. 11.491/2023. O art. 18, tal como ressaltado pelo Min. Gilmar Mendes, reforça o direito do Estado de ter “critérios adicionais de extensão da jurisdição”, abrangendo (i) a localização da pessoa jurídica que tem a posse ou o controle dos dados armazenados em um sistema informático e (ii) o fato de a pessoa jurídica fornecedora dos serviços de internet prestar o serviço no território daquele país” (STF, ADC 51, voto do Min. Relator Gilmar Mendes, j. 23-2-2023).

¹⁰ CARVALHO RAMOS, André de. **Curso de direitos humanos**. 12ª ed., São Paulo: Saraivajur, 2025, p. 842

¹¹ CARVALHO RAMOS, André de. **Curso de Direito Internacional Privado**. 4ª Ed. São Paulo: Saraiva, 2025, p. 569.

O tamanho maiúsculo do mercado digital brasileiro e o inegável engajamento do público nacional em diversas situações no mundo digital mostram que as plataformas digitais estrangeiras perdem muito na restrição ou suspensão de acesso ao mercado nacional (em 2022, o Brasil já era o 5º país com mais usuários de internet no mundo¹²).

Como destacam Carvalho Ramos e Abade, citando o voto do Min. Gilmar Mendes na ADC n. 51, o novo constitucionalismo digital dos Estados exige que os agentes econômicos respeitem as leis locais e as ordens judiciais, desconsiderando a alegação de armazenamento externo de dados, dada a natureza a-territorial do ambiente digital¹³.

Dessa forma, a decisão do STF reforça a capacidade do Poder Judiciário brasileiro de proteger direitos fundamentais no ambiente digital, mesmo diante da complexidade das relações internacionais e da resistência de algumas empresas de tecnologia em cumprir ordens judiciais proferidas no Brasil.

3 PROTEÇÃO DE DIREITOS E REGULAÇÃO DIGITAL: A DECISÃO DO STJ SOBRE A INDISPONIBILIDADE GLOBAL DE CONTEÚDO DIFAMATÓRIO

No Recurso Especial nº 2147711 - SP (2024/0065404-7), sob a relatoria da Ministra Nancy Andrighi, julgado em 12/11/2024 pela Terceira Seção do Superior Tribunal de Justiça (STJ), discutiu-se mais um aspecto envolvendo os efeitos extraterritoriais da jurisdição civil brasileira. O caso envolveu uma ordem judicial brasileira determinando que a empresa Google tornasse indisponível determinado conteúdo considerado flagrantemente ilícito (difamação com alto potencial de lesividade à empresa nacional do setor de alimentos) tanto no Brasil quanto no exterior.

No voto da relatora, destacou-se que determinada empresa brasileira do setor de alimentos, com mais de 50 anos de atuação e presença internacional, havia tomado conhecimento, em abril de 2014, de postagem de vídeo no YouTube, plataforma pertencente ao Google, com o título "Ratos encontrados em alimentos na empresa (*nome da empresa*)", publicado por um usuário.

Ainda conforme o voto da relatora, havia fortes indícios de falsidade do conteúdo do vídeo. Além da ausência de elementos visuais que corroborassem a acusação, a empresa de alimentos difamada comprovou estar em conformidade com as autoridades sanitárias. Diante disso, solicitou administrativamente a remoção do conteúdo, mas o pedido foi recusado pela plataforma, levando a empresa a ajuizar ação cautelar e, posteriormente, ação de obrigação de fazer cumulada com indenização por danos morais contra a filial brasileira do Google (Google Brasil Internet Ltda.).

O STJ ressaltou que a difamação era incontestável e não foi objeto de controvérsia por parte da recorrente, exceto quanto ao argumento de que o conteúdo poderia não ser considerado infrator em jurisdições estrangeiras. No entanto, a relatora ponderou que tal hipótese somente seria relevante se a recorrente demonstrasse, concretamente, um conflito entre o direito brasileiro

¹² Disponível em: <https://forbes.com.br/forbes-tech/2022/10/brasil-ja-e-o-5o-pais-com-mais-usuarios-de-internet-no-mundo/>. Acesso em 02 de janeiro de 2025

¹³ CARVALHO RAMOS, André de; ABADE, Denise Neves. Proteção de dados, soberania e imunidade tecnológica: impacto da ADC nº 51 na regulação de grandes empresas de internet pelo Brasil. **Revista Brasileira de Estudos Constitucionais**, v. 1, p. 49-70, 2023, em especial p. 70.

e o direito estrangeiro. Para isso, seria necessário seguir o rito da execução de sentença estrangeira e comprovar que a remoção do conteúdo afrontaria a soberania estrangeira. Dessa forma, o STJ não poderia emitir juízo abstrato sobre eventual violação da soberania de outros países.

Quanto ao alcance global da decisão judicial brasileira, a empresa de alimentos demonstrou que o conteúdo difamatório permanecia acessível fora do Brasil, como na Colômbia e na Alemanha. Tal circunstância evidenciava o risco de que a limitação territorial da indisponibilidade do vídeo tornaria incompleta a proteção jurisdicional de sua honra objetiva e reputação comercial.

No que se refere ao argumento de que o Judiciário brasileiro não teria jurisdição internacional para restringir o acesso de usuários ao conteúdo infrator em sites também estrangeiros, a relatora destacou que a própria Google Brasil Internet Ltda. reconheceu, em seu Relatório de Transparência, que atuavam removendo “links para um conteúdo considerado falso por um tribunal, inclusive em jurisdições além do mandado original” (transcrito do voto da Relatora).

Consequentemente, se a própria Google adota a política de remover conteúdos considerados falsos por tribunais sem que haja jurisdição direta sobre ela, a Relatora concluiu que não havia justificativa razoável para impedir que uma ordem judicial específica de indisponibilidade de conteúdo infrator tenha efeitos extraterritoriais, especialmente quando direcionada à filial brasileira da empresa.

A decisão do STJ reforçou que a ordem de indisponibilidade do conteúdo atende a interesses brasileiros (na defesa da ordem econômica brasileira – a empresa de alimentos vítima) e se fundamenta no ordenamento jurídico nacional. Assim, sua efetivação transfronteiriça decorre naturalmente da própria natureza global da internet. A relatora citou o Marco Civil da Internet (MCI), que define a rede mundial como um “sistema estruturado em *escala mundial*” (art. 5º, I, do MCI), o que justifica a possibilidade de proteção jurídica igualmente global.

Ademais, o voto destacou que, conforme o art. 19 do MCI, o “âmbito” dos serviços prestados pelos provedores de aplicações de internet é determinante: se o serviço é global, a ordem judicial de indisponibilidade também pode ter alcance global. O acórdão do STJ mencionou que ordens judiciais com efeitos extraterritoriais já são reconhecidas em diversas jurisdições, evidenciando uma tendência internacional de conferir maior efetividade à resolução de disputas que ultrapassam as fronteiras tradicionais.

Por essa razão, a relatora afastou qualquer ofensa, em tese, à soberania estrangeira, ao determinar a execução global da ordem judicial, uma vez que se trata de uma decisão cível que visa à proteção de direitos fundamentais previstos no ordenamento brasileiro.

Diante disso, o STJ decidiu manter integralmente o acórdão recorrido, confirmando a determinação de indisponibilidade global do conteúdo infrator identificado pelos URLs fornecidos pela empresa brasileira do setor de alimentos.

A decisão proferida pela Terceira Seção do Superior Tribunal de Justiça (STJ) representa um marco na afirmação da jurisdição civil brasileira sobre conteúdos ilícitos na internet, demonstrando sensibilidade à proteção da honra objetiva de empresas nacionais em um ambiente digital globalizado. Ao determinar a indisponibilidade do vídeo difamatório em nível mundial, o Tribunal garantiu que a proteção concedida pelo ordenamento jurídico brasileiro não fosse frustrada pela natureza descentralizada da internet.

O reconhecimento da necessidade de remoção extraterritorial não apenas preserva a reputação comercial da empresa lesada, mas também reafirma a jurisdição efetiva (e não somente

teorética) da Justiça brasileira em tutelar direitos fundamentais, alinhando-se a tendências internacionais de responsabilização de provedores de aplicação na internet. Além disso, a decisão mostra coerência com o próprio comportamento da Google, que já admite, em seu Relatório de Transparência, a remoção voluntária de conteúdos que foram considerados ofensivos ou ilícitos por outros tribunais estrangeiros, o que reforça a razoabilidade da ordem judicial brasileira.

Sob a ótica econômica, a decisão evita um efeito perverso que poderia resultar da exigência de remoção fragmentada e feita em cada jurisdição estrangeira. Se a proteção da honra objetiva da empresa fosse limitada ao território nacional, haveria um aumento expressivo dos custos jurídicos e operacionais para solicitar a exclusão do mesmo conteúdo em múltiplas jurisdições, especialmente considerando a existência de, no mínimo, 193 Estados no cenário internacional (membros da Organização das Nações Unidas).

Essa fragmentação poderia criar incentivos para uma competição desleal, permitindo que concorrentes explorassem lacunas regulatórias para difamar empresas em mercados estratégicos sem consequências efetivas. Assim, a solução adotada pelo STJ confere maior previsibilidade ao ambiente empresarial e assegura que a reputação de empresas brasileiras, com atuação internacional, não fique vulnerável a ataques que poderiam comprometer sua posição no mercado global.

4 A REGULAÇÃO JUDICIAL DOS PROVEDORES DE CONTEÚDO E O DEBATE SOBRE A RESPONSABILIZAÇÃO

O Supremo Tribunal Federal retomou, em dezembro de 2024, o julgamento sobre a constitucionalidade do artigo 19 do Marco Civil da Internet (Lei nº 12.965/2014) e a responsabilidade das plataformas digitais pelo conteúdo publicado por seus usuários (terceiros). Em um cenário onde as *big techs* desempenham um papel central na economia digital, a decisão do STF pode redefinir os limites da autonomia privada dessas empresas e a forma como elas gerenciam e moderam informações em ambientes virtuais.

O julgamento ocorre no contexto de dois recursos extraordinários com repercussão geral reconhecida: o RE nº 1.037.396, interposto pelo Facebook (Tema 987), e o RE nº 1.057.258, interposto pelo Google (Tema 533). Ambos discutem a responsabilidade civil dos provedores de aplicações de internet por danos decorrentes de conteúdos gerados por terceiros. O artigo 19 do Marco Civil estabelece que as plataformas só podem ser responsabilizadas civilmente caso descumpram uma ordem judicial específica para remoção de determinado conteúdo.

O embate jurídico contrapõe a visão das empresas, que alegam que o artigo protege a liberdade de expressão e evita remoções preventivas excessivas, à de grupos sociais que defendem uma maior responsabilização das plataformas diante da disseminação de conteúdos ilícitos.

Os votos dos Min. Toffoli e Min. Fux, relatores dos dois casos, caminharam na mesma direção, considerando inconstitucional o artigo 19 e propondo novas diretrizes para a responsabilização dos provedores. No entanto, o Min. Barroso apresentou uma posição intermediária, propondo uma interpretação mais flexível do artigo 19, sem sua total revogação por inconstitucionalidade, mas com a ampliação de exceções e novas obrigações regulatórias para as plataformas.

Ponto importante foi o destaque, logo no início da sessão, do presidente do STF, Min. Barroso, o qual apontou que o artigo 19 não protege “perfis falsos” ou “contas fake”.¹⁴ Após o voto do Min. Barroso, houve pedido de vista por parte do Min. André Mendonça.

4.1 O voto do Min. Toffoli: o fim da “imunidade” e a criação de um rol de condutas ilícitas

O primeiro voto foi proferido pelo Min. Toffoli, relator do RE nº 1.037.396, que defendeu a inconstitucionalidade do artigo 19 do Marco Civil da Internet¹⁵. Para o ministro, o dispositivo cria uma espécie de imunidade civil para as plataformas, já que a responsabilidade só surge caso uma decisão judicial não seja cumprida. Segundo o entendimento exposto, essa exigência deixa as vítimas desprotegidas, permitindo que conteúdos ilícitos permaneçam disponíveis por anos na internet (a depender da delonga da decisão judicial ou de seu trânsito em julgado) sem qualquer consequência para as plataformas.

Em substituição ao modelo atual, o Min. Toffoli propôs um novo critério de responsabilização, baseado na notificação extrajudicial pelo ofendido, sem necessidade de ordem judicial prévia, ampliando o alcance do artigo 21 do Marco Civil, que hoje se restringe à remoção de conteúdos relacionados a nudez ou atos sexuais privados. Além disso, o relator sugeriu uma lista taxativa de condutas que ensejariam a responsabilidade *objetiva* das plataformas, independentemente de notificação ou decisão judicial. Entre os conteúdos listados estão crimes contra o Estado democrático de Direito, atos de terrorismo, racismo, violência contra mulheres e crianças, tráfico de pessoas e divulgação de desinformação com impacto no processo eleitoral.

Outro ponto central do voto do Min. Toffoli foi a responsabilização das plataformas pela manutenção de contas inautênticas e pelo conteúdo impulsionado, seja por meio de anúncios pagos ou promovidos internamente. Com isso, as empresas passariam a ter o dever de monitorar ativamente a criação de perfis falsos e a veiculação de publicidade patrocinada, sob pena de responsabilidade solidária com o anunciante.

4.2 O voto do Min. Fux: remoção imediata e monitoramento ativo

Na sessão seguinte, o Min. Fux, relator do RE nº 1.057.258, também votou pela inconstitucionalidade do artigo 19, mas adotou uma abordagem ainda mais rigorosa. Em seu entendimento, a proteção da liberdade de expressão não pode justificar a propagação de conteúdos ilícitos, e as plataformas devem ser obrigadas a remover imediatamente postagens ofensivas assim que forem notificadas pelo usuário prejudicado.

Além disso, o Min. Fux também defendeu que, em determinados casos, a remoção deve ser feita sem necessidade de notificação prévia. Para o relator, conteúdos que veiculam discurso de ódio, racismo, pedofilia, incitação à violência e apologia à abolição violenta do Estado Democrático de Direito e ao golpe de Estado devem ser retirados do ar assim que forem identificados pelas plataformas, sem que haja a necessidade de um pedido formal por parte dos usuários.

¹⁴ Disponível em <https://www.jota.info/stf/do-supremo/artigo-19-o-que-dizem-especialistas-sobre-o-1o-dia-de-julgamento-no-stf>. Acesso em 02 de janeiro de 2025

¹⁵ Íntegra do voto disponível em <https://www.poder360.com.br/poder-justica/barroso-abre-divergencia-em-julgamento-sobre-responsabilizacao-de-redes/>. Acesso em 02 de janeiro de 2025

Essa abordagem impõe um “dever de cuidado”, retratado em monitoramento constante às plataformas, deslocando para as empresas os custos econômicos e a responsabilidade de identificar e moderar esses conteúdos antes mesmo de qualquer denúncia por parte dos usuários.

4.3 O voto do Min. Barroso: regulação, relatórios de impacto e dever de cuidado

O terceiro voto foi proferido pelo Min. Barroso, que divergiu parcialmente dos votos anteriores. Para o ministro, o artigo 19 do Marco Civil da Internet precisa ser reformulado (reinterpretado), mas não revogado integralmente. Inicialmente, o presidente do STF reconheceu que o artigo 19 do Marco Civil da Internet não oferece proteção adequada a direitos fundamentais, como a dignidade da pessoa humana, nem a princípios essenciais para a democracia.

Ele defendeu que algumas exceções já previstas no próprio Marco Civil (art. 21, visto acima) sejam ampliadas, permitindo a remoção de conteúdos sem ordem judicial prévia em situações mais abrangentes. Na visão do Min. Barroso, quando a plataforma recebe uma notificação sobre um conteúdo que configura crime evidente, como a criação de um perfil falso – caracterizado como crime de falsa identidade –, a remoção deve ocorrer sem a necessidade de intervenção judicial. Para ele, não há justificativa constitucional para um sistema que permita às plataformas permanecerem inertes diante de violações flagrantes da lei penal. Por outro lado, em casos mais subjetivos, como os crimes contra a honra, o Min. Barroso entende que a retirada de conteúdo deve ocorrer apenas mediante ordem judicial. Ainda que haja alegações de injúria, calúnia ou difamação, ele considera que a manutenção temporária da postagem é necessária para garantir a liberdade de expressão e evitar remoções indevidas. O controle judicial, segundo ele, é essencial para impedir censura indevida e assegurar que não haja o uso abusivo da legislação para silenciar indivíduos ou encobrir fatos de relevância pública que ainda estejam sob investigação¹⁶.

Além disso, o Min. Barroso propôs um modelo de regulação mais próximo do *Digital Services Act* (DSA) da União Europeia, com a exigência de relatórios anuais de impacto por parte das plataformas. Essas obrigações incluiriam a divulgação de ações para mitigar riscos sistêmicos, como a disseminação de desinformação, pornografia infantil, terrorismo e ataques à democracia.

O ministro também rejeitou a responsabilidade objetiva dos prestadores de aplicações da internet, argumentando que a responsabilização deve ser baseada na falha no dever de cuidado das empresas. Para o Min. Barroso, um erro isolado não deve ser suficiente para responsabilizar a plataforma, mas somente uma *falha sistêmica* na moderação de conteúdos justificaria sanções. Outra proposta apresentada foi a criação de um órgão regulador independente, com representantes do governo, empresas, sociedade civil e legislativo, para monitorar a atuação das *big techs* e aplicar sanções quando necessário¹⁷.

Ponto importante destacado pelo Ministro foi a preservação da separação de poderes. O Marco Civil da Internet foi construído no Poder Legislativo, em debates de anos. Para o Min. Barroso, o Legislativo tem um papel essencial na definição dos critérios regulatórios, mas que,

¹⁶ Disponível em <https://noticias.stf.jus.br/postsnoticias/marco-civil-da-internet-barroso-defende-que-plataformas-reduzam-riscos-de-postagens-criminosas/>. Acesso em 02 de janeiro de 2025

¹⁷ Disponível em <https://noticias.stf.jus.br/postsnoticias/marco-civil-da-internet-barroso-defende-que-plataformas-reduzam-riscos-de-postagens-criminosas/>. Acesso em 02 de janeiro de 2025

na ausência de uma lei específica, o STF deveria estabelecer regime jurídico apenas provisório. Ou seja, para o Min. Barroso, o “Marco Civil Judicial” serve como remédio temporário, mas a correção dos comportamentos deletérios vistos nos últimos anos deve ser incumbência do Legislativo¹⁸.

Após o voto do Min. Barroso, o Min. André Mendonça pediu vista.

4.4 Manifestações do Min. Alexandre de Moraes e do Min. Kássio Nunes

Durante a sessão, ministros que ainda votaram também se manifestaram¹⁹. O ministro Alexandre de Moraes contestou a alegação de que as plataformas digitais não teriam capacidade técnica para moderar o conteúdo postado pelos usuários, especialmente em casos de *cyberbullying*. Segundo ele, as empresas possuem plenas condições de identificar e controlar conteúdos como discursos racistas, manifestações nazistas e atos antidemocráticos. No entanto, apontou que a falta de ação decorre não de uma limitação tecnológica, mas sim de uma escolha deliberada das plataformas, que se beneficiam financeiramente da disseminação desse tipo de material²⁰.

Essa dimensão econômica da discussão trazida pelo Min. Moraes mostra a conseqüência não prevista da incidência regular do art. 19. O modelo de negócios das plataformas é beneficiado pelo engajamento e viralização de condutas ofensivas ou falsas. Por isso, não é racional confiar, cegamente, que o modelo de autorregulação atual e a atuação posterior (e tardia) do Poder Judiciário será eficiente para combater lesões a direitos.

Por outro lado, o ministro Kássio Nunes Marques expressou preocupações sobre o poder conferido às plataformas para decidir quais conteúdos devem ou não ser removidos, alertando para as consequências de torná-las árbritas do debate público. Ele argumentou que, ao se conferir um poder excessivo a essas empresas, há o risco de estabelecer um julgamento unilateral sobre o que é aceitável ou não, criando um ambiente de censura privada influenciado pelos interesses comerciais e ideológicos das próprias plataformas²¹.

4.5 Análise crítica

O debate no STF sobre a constitucionalidade do artigo 19 do Marco Civil da Internet demonstra uma análise sofisticada e equilibrada dos desafios contemporâneos da regulação das plataformas digitais.

O ministro Dias Toffoli destacou a necessidade de evitar um modelo que torne as plataformas imunes à responsabilização, permitindo que a viralização de conteúdos ilícitos cause danos irreparáveis antes que o Judiciário possa intervir. Como bem anotado pelo Min. Fux, a exigência de decisão judicial de remoção revela “proteção deficiente”, uma vez que a conduta ilícita “viraliza em minutos, em horas, e para o mundo em horas”. Para o Min. Fux, o modelo do artigo

¹⁸ Disponível em <https://noticias.stf.jus.br/postsnoticias/marco-civil-da-internet-barroso-defende-que-plataformas-reduzam-riscos-de-postagens-criminosas/>. Acesso em 02 de janeiro de 2025

¹⁹ Disponível em <https://www.jota.info/stf/do-supremo/barroso-considera-artigo-19-do-mci-parcialmente-inconstitucional-mendonca-pede-vista>. Acesso em 02 de janeiro de 2025.

²⁰ Disponível em <https://www.jota.info/stf/do-supremo/barroso-considera-artigo-19-do-mci-parcialmente-inconstitucional-mendonca-pede-vista>. Acesso em 02 de janeiro de 2025.

²¹ Disponível em <https://www.jota.info/stf/do-supremo/barroso-considera-artigo-19-do-mci-parcialmente-inconstitucional-mendonca-pede-vista>. Acesso em 02 de janeiro de 2025.

19 resulta em “justiça tardia”, a qual transforma a reparação em um “prêmio de consolação”, sem nenhum efeito preventivo²².

Essa perspectiva reforça o entendimento de que a responsabilização judicial posterior, nos moldes atuais, é insuficiente para lidar com a velocidade da disseminação digital e a magnitude dos impactos causados (de alcance global). Ao reconhecer a ineficiência desse modelo, o Tribunal avança na construção de uma solução que contemple tanto a proteção dos direitos fundamentais quanto a funcionalidade da internet como espaço democrático.

Por outro lado, as preocupações manifestadas pelo ministro Barroso são igualmente relevantes para garantir que um novo regime de responsabilidade para as plataformas não resulte em censura indevida ou em um arbítrio excessivo por parte das empresas. Seu entendimento de que crimes contra a honra devem ser avaliados judicialmente antes da remoção demonstra uma sensibilidade importante ao direito à liberdade de expressão e ao risco de remoções precipitadas. Ao mesmo tempo, a proposta de um órgão colegiado e da reserva do Parlamento (a solução judicial – o “Marco Civil Judicial” do título deste artigo seria provisória) para lidar com esses conflitos de interesse sugere um caminho intermediário que pode evitar tanto a inação das plataformas quanto a adoção de critérios opacos e potencialmente enviesados.

Assim, o que tem sido debatido no STF sinaliza um avanço regulatório que não apenas enfrenta as limitações do modelo atual, mas também busca evitar excessos em qualquer direção.

O reconhecimento da necessidade de uma atuação mais ágil contra conteúdos manifestamente ilícitos, somado à preocupação com a liberdade de expressão e à busca por soluções institucionais para a moderação de conteúdos, demonstra que o STF está em busca de uma resposta ponderada. A definição de critérios objetivos e a criação de mecanismos de controle mais eficientes podem garantir que a internet continue sendo um espaço plural e democrático, sem que os direitos fundamentais fiquem reféns de interesses privados ou de processos judiciais excessivamente morosos.

CONCLUSÃO: OS DELINEAMENTOS DO MARCO CIVIL JUDICIAL DA INTERNET E A ECONOMIA DIGITAL

A evolução da interpretação do Marco Civil da Internet à luz dos casos paradigmáticos vistos acima reflete um esforço contínuo do Poder Judiciário brasileiro para compatibilizar a proteção de direitos fundamentais com a regulação da economia digital.

As decisões analisadas demonstram uma crescente densificação da tutela jurisdicional, garantindo que as plataformas digitais não operem à margem da responsabilidade civil e da soberania estatal. A definição de critérios objetivos para a remoção de conteúdos ilícitos, bem como a possibilidade de alcance extraterritorial (global) de ordens judiciais brasileiras, fortalece a proteção da honra, da privacidade e da integridade informacional no ambiente digital, ao mesmo tempo em que estabelece um ambiente mais previsível para a atuação das empresas.

Esse avanço regulatório se alinha a tendências internacionais que buscam reequilibrar o poder das *big techs* e evitar que a arquitetura digital favoreça práticas que geram externalidades negativas à sociedade e promovam a economia digital e modelos de negócios que estimulam viralização e monetizações à custa de direitos.

²² Disponível em <https://www.jota.info/stf/do-supremo/fux-acompanha-toffoli-na-inconstitucionalidade-do-artigo-19-e-barroso-pede-vista> Acesso em 02 de janeiro de 2025

O debate travado no Supremo Tribunal Federal e a proposta de um “Marco Civil Judicial” temporário demonstram que essa regulação não pode ser responsabilidade exclusiva do Poder Judiciário. O compromisso com a liberdade de expressão e a necessidade de evitar censura privada ou estatal excessiva exigem que a sociedade civil e o Parlamento assumam um papel central na definição dos parâmetros para a responsabilização das plataformas.

A experiência de elaboração do Marco Civil da Internet, marcada pela ampla participação social e pelo espírito plural, deve ser resgatada para que eventuais alterações legislativas mantenham esse equilíbrio essencial.

Além disso, a criação de um órgão colegiado com representação democrática para tratar de conflitos envolvendo a moderação de conteúdos pode ser uma solução institucional adequada para evitar a judicialização excessiva e a tomada de decisões baseadas em interesses privados ou ideológicos.

Dessa forma, o que se observa não é um deslocamento radical do modelo regulatório originalmente previsto no Marco Civil da Internet, mas sim sua adaptação a um cenário digital que se transformou substancialmente desde 2014.

O fortalecimento da jurisdição brasileira diante da resistência dos provedores de aplicação e a responsabilização proporcional das plataformas representam avanços necessários para que o ambiente digital seja mais seguro e democrático. No entanto, esse processo não pode ocorrer sem um amplo diálogo entre os Poderes e a sociedade, garantindo que a regulação digital no Brasil continue sendo marcada pelo pluralismo e pela preservação dos direitos fundamentais.

REFERÊNCIAS

CARVALHO RAMOS, André de; ABADE, Denise Neves. Proteção de dados, soberania e imunidade tecnológica: impacto da ADC nº 51 na regulação de grandes empresas de internet pelo Brasil. **Revista Brasileira de Estudos Constitucionais**, v. 1, p. 49-70, 2023.

CARVALHO RAMOS, André de. **Curso de Direito Internacional Privado**. 4ª Ed. São Paulo: Saraiva, 2025.

CARVALHO RAMOS, André. **Curso de direitos humanos**. 12ª ed., São Paulo: Saraivajur, 2025.

CARVALHO, Patrícia Heloisa de. O “Marco Civil da Internet”: uma análise sobre a constitucionalidade do artigo 19. **Revista da Faculdade de Direito do Sul de Minas**, v. 33, n.2 p. 228-244, 2017.

LIMA, Cíntia Rosa Pereira de. A responsabilidade civil dos provedores de aplicação de internet por conteúdo gerado por terceiro antes e depois do Marco Civil da Internet (Lei n. 12.965/14). **Revista da Faculdade de Direito, Universidade de São Paulo**, v. 110, p. 155-176, 2015.

SOUZA, Carlos Affonso; LEMOS, Ronaldo. **Marco civil da internet: construção e aplicação**. Juiz de Fora: Editar, 2016.

TEFFÉ, Chiara Spadaccini de; MORAES, Maria Celina Bodin de. Redes sociais virtuais: privacidade e responsabilidade civil. Análise a partir do Marco Civil da Internet. **Pensar**, Fortaleza, v. 22, n. 1, p. 108-146, jan./abr. 2017.

THOMPSON, Marcelo. Marco Civil ou Demarcação de Direitos? Democracia, Razoabilidade e as Fendas na Internet do Brasil. **Revista de Direito Administrativo**, v. 261, p. 203-251, 2012

Marco civil judicial da internet: promovendo direitos e responsabilização na nova ordem econômica digital

TOMASEVICIUS FILHO, Eduardo. Marco Civil da Internet: uma lei sem conteúdo normativo. **Estudos Avançados**, v. 30, p. 269-285, 2016.