

Autores

Carolina Adler Cendron
Eduardo Serra Rossigneux Vieira
Fernanda Campos Botelho
Fernanda dos Santos Rodrigues Silva
Fernanda Sathler Rocha Franco
Gabriella da Silva Reis
Giovanni Simão Triginelli
Helena Penna Marchi
Henrique Almeida Bazan
Inma Conde
Jéssica Fernandes Rocha
José Luiz de Moura Faleiros Júnior
Laurence Duarte Araújo Pereira
Leonardo Andrade Macedo
Lorenzo Antonini Itabaiana
Maelle Antunes Pereira Lima
Maria Cláudia Viana Hissa Dias do Vale Gangana
Natália Cristina Chaves

Leonardo **PARENTONI**

Coordenador

Fernanda Campos **Botelho**
Fernanda Sathler Rocha **Franco**
Giovanni Simão **Triginelli**
Laurence Duarte Araújo **Pereira**

Organização



DIREITO, TECNOLOGIA E INOVAÇÃO

vol. 7: 10 anos do Marco Civil da Internet



“O presente volume enfoca os *10 anos do Marco Civil da Internet*, tecnicamente a Lei n. 12.965, de 23 de abril de 2014. Dotada de importância estrutural para o funcionamento da internet no Brasil, coube a ela regular temas como os fundamentos do uso da internet, direitos e garantias dos usuários, deveres e responsabilidade civil dos provedores de serviços na internet, neutralidade de rede, alguns aspectos sobre proteção de dados pessoais e, ainda, o polêmico tópico da moderação de conteúdo online, coloquialmente rotulado como “regulação de plataformas” ou “regulação de redes sociais”.

Este livro é fruto, em parte, da disciplina de mesmo nome lecionada na Faculdade de Direito da UFMG, em 2024. Posteriormente complementado e expandido com a contribuição de especialistas convidados, nacionais e estrangeiros, das mais diversas áreas de atuação, como por exemplo, Magistério, Advocacia e Ministério Público. O propósito da obra foi refletir sobre como tem sido interpretado e aplicado o Marco Civil da Internet (doravante apenas “MCI”), uma década após a sua entrada em vigor. A fim de identificar se os principais objetivos desta lei foram realmente alcançados (e em que medida), bem como se o MCI seria capaz de solucionar os novos desafios, no todo ou em parte. Por fim, identificando a necessidade de eventual alteração legislativa.

(...)

Com efeito, este volume contém 13 ensaios, agrupados por tema ao longo de 06 partes. A Parte I versa sobre o papel do MCI no constitucionalismo digital, a partir de texto de Inma Conde, autora estrangeira convidada da Universidade de Sydney/Austrália.

Na sequência, a Parte II trata da perícia forense computacional, com base em dois ensaios de profissionais que atuam com esse tema, a saber: Leonardo Macedo, do Ministério Público Federal, e Jéssica Rocha, advogada.

A Parte III, por sua vez, trata da neutralidade de rede, um dos alicerces do MCI, enfocando tanto os seus aspectos computacionais e jurídicos quanto a questão concorrencial do “*fair share*”.

A Parte IV dedica-se ao estudo dos provedores de serviços na internet (ISPs), abordando assuntos como a sua classificação, dever de armazenar logs/registros, regime de responsabilidade civil e evolução da jurisprudência. Na Parte V estão reunidos alguns ensaios específicos sobre moderação de conteúdo online, um dos deveres dos ISPs que se optou por destacar em tópico separado, tendo em vista a complexidade e controvérsia do tema. Este ponto da obra compreende estudos de perfil crítico analisando desde a intenção original do MCI até a recente decisão do STF, já mencionada anteriormente, além da diminuição proposital do alcance de certos conteúdos (“*shadow baning*”).

Conclui-se a obra com a Parte VI, que contém análise de perfil crítico/filosófico, em coautoria de três pesquisadores, sobre o que de fato está em jogo quando se discute a moderação de conteúdo online, partindo da premissa de que moderar conteúdo alheio é uma forma de exercício de poder”.

Trecho do Prefácio do Coordenador LEONARDO PARENTONI

DIREITO, TECNOLOGIA E INOVAÇÃO

vol. 7: 10 anos do Marco Civil da Internet



A presente obra foi publicada sob os direitos da Creative Commons 4.0 BY-SA. Mais informações em:
<https://creativecommons.org/licenses/by-sa/4.0/>

Autores

Carolina Adler Cendron
Eduardo Serra Rossignaux Vieira
Fernanda Campos Botelho
Fernanda dos Santos Rodrigues Silva
Fernanda Sathler Rocha Franco
Gabriella da Silva Reis
Giovanni Simão Triginelli
Helena Penna Marchi
Henrique Almeida Bazan
Inma Conde
Jéssica Fernandes Rocha
José Luiz de Moura Faleiros Júnior
Laurence Duarte Araújo Pereira
Leonardo Andrade Macedo
Lorenzo Antonini Itabaiana
Maelle Antunes Pereira Lima
Maria Cláudia Viana Hissa Dias do Vale Gangana
Natália Cristina Chaves

Leonardo **PARENTONI**

Coordenador

Fernanda Campos **Botelho**
Fernanda Sathler Rocha **Franco**
Giovanni Simão **Triginelli**
Laurence Duarte Araújo **Pereira**

Organização



DIREITO TECNOLOGIA E INOVAÇÃO

vol. 7: 10 anos do Marco Civil da Internet



DIREITO, TECNOLOGIA E INOVAÇÃO – V. 7:
10 ANOS DO MARCO CIVIL DA INTERNET

Coordenação	Leonardo Parentoni
Conselho Editorial Institucional	Brazilian Journal of Law, Technology and Innovation
Equipe de Organização deste Volume	Fernanda Campos Botelho Fernanda Sathler Rocha Franco Giovanni Simão Triginelli Laurence Duarte Araújo Pereira
Capa	Equipe Editorial
Publicação	Centro de Pesquisa em Direito, Tecnologia e Inovação – Centro DTIBR
Diagramação	Equipe Editorial



Centro de Pesquisa em Direito, Tecnologia e Inovação – Centro DTIBR
CNPJ/MF nº 32.727.924/0001-80
Rua dos Timbiras, 1925, Sala 903, Lourdes, Belo Horizonte/MG, Brasil
CEP 30140-069
www.dtibr.com

Todos os direitos reservados.
Fechamento da edição: 08/2025.

Dados Internacionais de Catalogação na Publicação (CIP)

-
- D598 Direito, Tecnologia e Inovação – v. VII: 10 anos do Marco Civil da Internet / Leonardo
2025 Parentoni [coordenador]; Fernanda Campos Botelho, Fernanda Sathler Rocha Franco,
Giovanni Simão Triginelli, Laurence Duarte Araújo Pereira [organizadores]. Belo Horizonte:
Centro DTIBR, 2025.
458 p.
Inclui bibliografia.
Obra coletiva. Vários autores.
ISBN: 978-65-998370-3-6
DOI: <https://doi.org/10.59224/dti7>
Ilustração da capa: rawpixel.com / Freepik (CC-BY)
1. Direito. 2. Direito digital. 3. Direito, tecnologia e inovação. I. Parentoni, Leonardo. II.
Botelho, Fernanda Campos. III. Franco, Fernanda Sathler Rocha. IV. Triginelli, Giovanni
Simão. V. Pereira, Laurence Duarte Araújo.

CDU: 340/CDD: 342.2

“(...) Marco Civil da Internet é, como dito, um direcionamento para os debates futuros. Integrando o ordenamento jurídico e indicando regimes de proteção de dados e de responsabilização, é fácil perceber o impacto do texto legal no Poder Judiciário, a quem cabe aplicar muitas das suas disposições.

Mas é preciso ir além e entender que o impacto do Marco Civil vai além das demandas judiciais, dos debates doutrinários e que o seu destinatário final é cada brasileiro que se vale da rede para os mais diversos fins. Garantir que a rede continue sendo um espaço aberto e promotor de liberdades é a função maior da Lei nº 12.965/2014.

Esse objetivo apenas poderá ser cumprido caso exista um acompanhamento constante sobre a aplicação de seus dispositivos e o escrutínio rigoroso das tentativas de modificação do texto que podem sabotar a sua missão principal.”.

CARLOS AFFONSO SOUZA E RONALDO LEMOS
Marco Civil da Internet: Construção e Aplicação (2016)

Aos habituais e novos leitores, o Centro DTIBR tem a felicidade de apresentar o sétimo volume de sua tradicional coletânea intitulada “Direito, Tecnologia e Inovação”, pioneira no país quanto à linha dogmática de mesmo nome. Recordando que todos os volumes anteriores podem ser acessados, gratuitamente, no site do Centro DTIBR (www.dtibr.com), na aba “Publicações”. Assim como no perfil do Professor Leonardo Parentoni, na plataforma ResearchGate.

O presente volume enfoca os *10 anos do Marco Civil da Internet*, tecnicamente a Lei n. 12.965, de 23 de abril de 2014. Dotada de importância estrutural para o funcionamento da internet no Brasil, coube a ela regular temas como os fundamentos do uso da internet, direitos e garantias dos usuários, deveres e responsabilidade civil dos provedores de serviços na internet, neutralidade de rede, alguns aspectos sobre proteção de dados pessoais e, ainda, o polêmico tópico da moderação de conteúdo *online*, coloquialmente rotulado como “regulação de plataformas” ou “regulação de redes sociais”.

Este livro é fruto, em parte, da disciplina de mesmo nome lecionada na Faculdade de Direito da UFMG, em 2024¹. Posteriormente complementado e expandido com a contribuição de especialistas convidados, nacionais e estrangeiros, das mais diversas áreas de atuação, como por exemplo, Magistério, Advocacia e Ministério Público. O propósito da obra foi refletir sobre como tem sido interpretado e aplicado o Marco Civil da Internet (doravante apenas “MCI”), uma década após a sua entrada em vigor. A fim de identificar se os principais objetivos desta lei foram realmente alcançados (e em que medida), bem como se o MCI seria capaz de solucionar os novos desafios, no todo ou em parte. Por fim, identificando a necessidade de eventual alteração legislativa.

1. Na área de estudos denominada “Direito, Tecnologia e Inovação: Análise científica e multidisciplinar da inovação tecnológica”. Maiores informações em: <<https://pos.direito.ufmg.br/projetos-coletivos/>>. Acesso em: 17 jul. 2025.

Felizmente, o momento não poderia ser mais oportuno para (re)estudar o tema. Afinal, o MCI é uma das principais fontes normativas brasileiras sobre moderação de conteúdo *online*, tema polêmico e que vem sendo muito debatido, tanto na mídia quanto na literatura especializada e nos tribunais. Não raras vezes, de forma atécnica, açodada, guiada por vieses ideológicos e desconsiderando (ou seria desconhecendo?) a profícua trajetória histórica que culminou na edição do MCI, após longos e aprofundados debates.

Afinal, é sempre bom lembrar a coincidência de que esta lei – cujo principal escopo é regular o uso da internet – foi justamente a *primeira* lei do Brasil em que se permitiu o envio de comentários e críticas *diretamente* pela rede mundial de computadores, tendo recebido mais de *duas mil sugestões*², provenientes de inúmeros segmentos da sociedade brasileira. Ou seja, o processo legislativo que culminou no MCI foi muito, mas muito além das etapas tradicionais, a cargo do Congresso Nacional. Ele foi um exemplo de participação democrática direta, inclusive com *repercussão mundial*³.

Sendo que um dos pontos mais debatidos do MCI, à época, foi justamente a moderação de conteúdo. Como (feliz ou infelizmente) não se pode ter tudo ao mesmo tempo, foi preciso refletir e conciliar as várias visões divergentes para alcançar, senão a unanimidade, ao menos um consenso que pudesse ser consagrado na lei. Havia, à época, a necessidade de harmonizar dois valores igualmente importantes, porém muitas vezes conflitantes em casos concretos: de um lado, a liberdade de expressão, que pressupõe a internet aberta, participativa e plural⁴; de outro lado, a preocupação

-
2. Descrevendo detalhadamente o processo legislativo do MCI, vide: SOUZA, Carlos Affonso Pereira de; LEMOS, Ronaldo. *Marco Civil da Internet: Construção e Aplicação*. Juiz de Fora: Editar, 2016. p. 20 e seguintes.
 3. Itália, França e outros países expressamente mencionaram a influência do MCI brasileiro em sua regulação interna. No mesmo sentido registrou a literatura técnica: SALDÍAS, Osvaldo. Coded for Export! The Contextual Dimension of the Brazilian Marco Civil da Internet. *Alexander von Humboldt Discussion Paper 2014-06*. p. 01-24, Nov. 2014. p. 02 “Marco Civil da Internet has an implicit global ambition in that it was conceived as a possible template for global regulation.”
 4. Haveria um dever de se manter a internet aberta e apta a possibilitar o maior número possível de manifestações, das mais diferentes espécies e pontos de vista. Algo já destacado em obras de

sobre como coibir eventuais abusos que inevitavelmente ocorreriam e de que forma deveria ser feita a remoção compulsória de conteúdo. A primeira corrente defendia que a legitimidade para identificar o que é ou não ilícito deveria caber exclusivamente ao Poder Judiciário, por ser o magistrado, presumivelmente, um terceiro imparcial que não permitiria a retirada de conteúdo para fins de censura ou outros interesses ilícitos. Portanto, salvo circunstâncias excepcionais (expressamente previstas em leis esparsas ou no próprio MCI art. 21, por exemplo), toda remoção de conteúdo dependeria de *prévia* decisão judicial. A opção oposta seria impor ao provedor de serviços na internet (internacionalmente conhecido pela sigla “ISP”) o dever de remover conteúdo gerado por terceiros sempre que recebesse notificação direta da parte interessada, sem necessidade de ordem judicial alguma. Este sistema ficou conhecido como notificação e retirada (“*notice and take down*”⁵), porque basta a notificação para acarretar o dever de remoção do conteúdo.

No projeto de lei, a versão original do MCI inclinava-se para o *notice and take down*. Entretanto, durante as consultas públicas (recorde-se que houve efetiva participação da sociedade brasileira) ficou clara a preocupação com a provável censura por parte dos ISPs. Afinal, seria menos arriscado para eles simplesmente remover qualquer conteúdo, ao ser notificado pela parte interessada, do que não o remover e, com isso, assumir para si o ônus de ser pessoalmente responsabilizado na hipótese de haver posterior discussão judicial do tema, na qual o conteúdo não removido

referência internacional, como “*free culture*” e “*remix*”: LESSIG, Lawrence. *Free Culture: The Nature and Future of Creativity*. New York: Penguin Books, 2005; e LESSIG, Lawrence. *Remix: Making Art and Commerce Thrive in the Hybrid Economy*. London: Bloomsbury Academic, 2008.

5. Mais recentemente, optou-se pelo termo “notificação e ação” (*notice and action*), porque ao ser notificado pela parte interessada o ISP pode adotar diversas condutas, que vão muito além de simplesmente manter ou excluir todo o conteúdo. Pode, por exemplo, ampliar ou reduzir o seu alcance, sinalizá-lo de forma destacada, solicitar esclarecimentos a respeito, buscar a conciliação, suspender temporariamente, etc.

Neste sentido se posicionou a União Europeia, ao regular o tema nos artigos 16 a 23 do *Digital Services Act*: EUROPEAN UNION. European Commission. *Proposal for a Regulation on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC n° 2016/679/CE*. Brussels: 15 Dec. 2020. Available at: <<https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A825%3AFIN>>. Access: 06 Oct. 2022.

viesse a ser declarado ilícito. Por esta razão o MCI foi alterado, durante o processo legislativo, para consagrar o sistema de ordem judicial prévia. Ou seja, o ISP somente poderia ser pessoalmente responsabilizado em caso de descumprimento desta ordem judicial, e não porque se recusou a remover conteúdo de terceiro, a partir de mera notificação da parte interessada. Disso resultou a redação original do art. 19, *caput*, em 2014:

“Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário.”

Perceba-se que ao invés de simplesmente consignar qual é a regra jurídica, pura e simples, o citado art. 19 teve o cuidado de registrar também os *fundamentos* com base nos quais o legislador chegou àquela conclusão: *“com o intuito de assegurar a liberdade de expressão e impedir a censura”*. Frise-se: o legislador da época fez uma opção expressa, refletida e muito bem fundamentada.

Uma década após a entrada em vigor do MCI, o panorama brasileiro e mundial já havia se modificado consideravelmente. É notório que as redes sociais⁶ hoje desempenham papel importante na sociedade, sendo a principal fonte de informação e conteúdo para milhões de pessoas⁷. O aumento e pulverização das fontes de consulta trouxe consigo novos problemas, como desinformação (*“fake news”*), manipulação

6. GRAEF, Inge. Mandating portability and interoperability in online social networks: regulatory and competition law issues in the European Union. *Telecommunications Policy*. Amsterdam: Elsevier. v. 39, n. 06, p. 502-514, Jul. 2015. p. 504. “(...) social networks are understood as services enabling users to create a public or semi-public profile and a list of friends or contacts.”

7. Alguns estudos da Universidade de Tecnologia de Sydney (UTS), feitos por instituição especializada na área jornalística (*Centre For Media Transition*), apontam que grande parte do público busca conteúdo jornalístico exclusivamente nas redes sociais, em detrimento de fontes clássicas como jornais, rádio e TV. Vide: <https://www.uts.edu.au/research/centres/centre-media-transition/publications>

comportamental e discursos de ódio. Neste novo contexto, o melhor caminho seria que o próprio Poder Legislativo, após consultar novamente a sociedade brasileira, decidisse por manter ou alterar o MCI, para adaptá-lo aos novos tempos. Não foi, porém, o que de fato aconteceu...

Em 2021, o governo do então Presidente Jair Bolsonaro editou uma medida provisória⁸ para reforçar a observância do sistema de ordem judicial prévia, já previsto na versão original do MCI. Acompanhada da seguinte exposição de motivos:

“O Marco Civil da Internet prevê que o uso da internet no Brasil deve observar, entre outros, os princípios da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal. E, ainda, declara expressamente que a garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet, sendo nulas de pleno direito as cláusulas contratuais que violem tal disposição.

No entanto, a previsão abstrata desses direitos e garantias tem se mostrado insuficiente para evitar que um número crescente de brasileiros tenha suas contas ou conteúdos removidos de maneira unilateral, arbitrária e imotivada por provedores de redes sociais, que, ao assim agirem, violam frontalmente o ordenamento jurídico brasileiro. Em grande parte dos casos, os usuários afetados por decisões arbitrárias de moderação de conteúdo não encontram, junto ao provedor, recurso célere para impedir ou fazer cessar a violação de seus direitos.”

Ocorre que essa medida provisória nunca foi convertida em lei e, com isso, perdeu totalmente a eficácia. Com efeito, ela foi imediatamente devolvida pelo Congresso Nacional⁹, ao argumento de que o tema deveria ser enfrentado pelo próprio Poder Legislativo, via tramitação regular dos projetos de lei em curso, e não por decisão unilateral do Chefe do Poder Executivo, como se pretendeu fazer à época.

Fato é que durante a disputa entre Executivo e Legislativo pelo “protagonismo” no tema, a constitucionalidade do art. 19 do MCI passou a ser discutida também no âmbito judicial, mais especificamente no Supremo Tribunal Federal¹⁰. Após um

8. Medida Provisória n. 1.068, de 06 de setembro de 2021.

9. Vide Ato Declaratório do Presidente da Mesa do Congresso Nacional n. 58, de 2021.

10. STF, Plenário, RE. n.º 1.037.396/SP, j. 27.06.2025, Rel. Ministro Dias Toffoli; e STF, Plenário, RE.

julgamento bastante controvertido, em que foram veiculadas pelo menos 04 teses jurídicas distintas (e, eventualmente, até incompatíveis)¹¹, por 08 votos contra 03 o Pleno do STF decidiu pela *inconstitucionalidade parcial e progressiva* do art. 19 do MCI e, conseqüentemente, do sistema de ordem judicial prévia. Reconhecendo expressamente que esta decisão judicial instaura um regime jurídico *provisório*, vigente apenas até que o Congresso Nacional – que é o maior legitimado para decidir a respeito – promova as alterações que julgar necessárias no MCI. Fato é que a decisão do STF inaugurou um sistema ainda mais controverso e totalmente distinto do que estava contido no MCI, como será detalhado e aprofundado ao longo de vários capítulos desta obra.

Feita essa breve contextualização do tema e da contemporaneidade desta obra, passo a discorrer brevemente sobre qual é a sua estrutura, de modo a proporcionar ao leitor uma visão panorâmica do livro. Com efeito, este volume contém 13 ensaios, agrupados por tema ao longo de 06 partes. A *Parte I* versa sobre o *papel do MCI no constitucionalismo digital*, a partir de texto de Inma Conde, autora estrangeira convidada da Universidade de Sydney/Austrália.

Na sequência, a *Parte II* trata da *perícia forense computacional*, com base em dois ensaios de profissionais que atuam com esse tema, a saber: Leonardo Macedo, do Ministério Público Federal, e Jéssica Rocha, advogada.

A *Parte III*, por sua vez, trata da *neutralidade de rede*, um dos alicerces do MCI, enfocando tanto os seus aspectos computacionais e jurídicos quanto a questão concorrencial do “*fair share*”.

A *Parte IV* dedica-se ao estudo dos *provedores de serviços na internet* (ISPs), abordando assuntos como a sua classificação, dever de armazenar *logs*/registros, regime de responsabilidade civil e evolução da jurisprudência. Na *Parte V* estão reunidos

n.º 1.057.258/SP, j. 27.06.2025, Rel. Ministro Luiz Fux.

11. Para um resumo das diversas teses jurídicas examinadas pelo STF, consulte-se: MULHOLLAND, Caitlin; AYALA, Marcelo. STF e o julgamento acerca da constitucionalidade do art. 19, do marco civil da internet. *Migalhas de Responsabilidade Civil*. 15 jul. 2025. Disponível em: <<https://www.migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/434569/stf-julga-a-constitucionalidade-do-art-19-do-marco-civil-da-internet>>. Acesso em: 21 jul. 2025.

alguns ensaios específicos sobre moderação de conteúdo *online*, um dos deveres dos ISPs que se optou por destacar em tópico separado, tendo em vista a complexidade e controvérsia do tema. Este ponto da obra compreende estudos de perfil crítico analisando desde a intenção original do MCI até a recente decisão do STF, já mencionada anteriormente, além da diminuição proposital do alcance de certos conteúdos (“*shadow banning*”).

Conclui-se a obra com a *Parte VI*, que contém análise de perfil crítico/filosófico, em coautoria de três pesquisadores, sobre o que de fato está em jogo quando se discute a moderação de conteúdo *online*, partindo da premissa de que moderar conteúdo alheio é uma forma de exercício de *poder*. Assim, *quanto mais deveres de moderação se atribuir a um ISP – queira-se ou não – mais isso acarretará aumento dos seus poderes* e, conseqüentemente, de sua capacidade para influenciar a sociedade e a economia, como já havia alertado Eugene Volokh¹².

Encerra-se o prefácio citando novamente a frase de Carlos Affonso e Ronaldo Lemos, destacada no preâmbulo deste livro, por ser uma feliz síntese da finalidade maior do MCI e dos riscos que se deve evitar ao alterá-lo:

“(...) o seu destinatário final é cada brasileiro que se vale da rede para os mais diversos fins. Garantir que a rede continue sendo um espaço aberto e promotor de liberdades é a função maior da Lei nº 12.965/2014.

Esse objetivo apenas poderá ser cumprido caso exista um acompanhamento constante sobre a aplicação de seus dispositivos e o escrutínio rigoroso das tentativas de

12. VOLOKH, Eugene. The Reverse Spider-Man Principle: With Great Responsibility Comes Great Power. *Journal of Free Speech Law*. Los Angeles: Journal of Free Speech Law. v. 03, n. 01, p. 197-216, 2023. p. 197-198. “Some of those customers are using the entity’s services in ways that are criminal, tortious, or otherwise reprehensible. Should the entity be held responsible, legally or morally, for its role (however unintentional) in facilitating its customers’ activities?”

(...)

I’d like to focus on one downside of answering it ‘yes’: what I call *the Reverse Spider-Man Principle* - *with great responsibility comes great power*. Whenever we are contemplating holding entities responsible for their customers’ behavior, we should think about whether we want to empower such entities to surveil, investigate, and police their customers (...).”

modificação do texto que podem sabotar a sua missão principal.”¹³

Que tanto a interpretação do MCI quanto suas eventuais alterações tenham como premissa preservar os valores centrais que historicamente motivaram a criação da lei: garantir uma internet de alcance mundial, aberta, colaborativa, diversificada, com liberdade de iniciativa e de opinião. Acima de tudo, assegurar que a internet não seja instrumentalizada por qualquer governo ou espectro ideológico.

Belo Horizonte/MG, agosto de 2025.

LEONARDO PARENTONI

Doutor em Direito Comercial pela USP. Professor da Faculdade de Direito da UFMG e do IBMEC/MG. Coordenador do Grupo de Trabalho em IA e Direito do Consórcio de Faculdades de Direito do BRICS. Ex-Conselheiro da composição original do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPd), nomeado pela Presidência da República. Fundador e Coordenador do projeto coletivo em Direito, Tecnologia e Inovação na Pós-Graduação da Faculdade de Direito da UFMG. Procurador Federal/AGU.

13. SOUZA, Carlos Affonso Pereira de; LEMOS, Ronaldo. *Marco Civil da Internet: Construção e Aplicação*. Juiz de Fora: Editar, 2016. p. 150.

Centro de Pesquisa em Direito, Tecnologia e Inovação – Centro DTIBR

O Centro de Pesquisa em Direito, Tecnologia e Inovação - Centro DTIBR é uma associação sem fins econômicos, composta por equipe multidisciplinar, com o propósito de conectar o meio acadêmico e a iniciativa privada, para o treinamento de pessoas e a disseminação de conteúdo, bem como o desenvolvimento de produtos e serviços inovadores na área de Direito e Tecnologia. Sempre mantendo o compromisso com a profundidade científica das atividades e o respeito aos mais elevados padrões éticos. Conheça mais a respeito no site (<https://www.dtibr.com/>) ou no Facebook (<https://www.facebook.com/CentroDTIBR/>), Instagram (<https://www.instagram.com/centrodtibr/>) e LinkedIn (<https://pt.linkedin.com/company/centrodtibr>).

Breves currículos dos coordenadores e dos autores

Coordenador

Leonardo Parentoni

Tem mais de 20 anos de experiência nos setores público e privado. É Doutor em Direito pela USP. Mestre em Direito Empresarial pela UFMG. Especialista em Direito Processual Civil pela UnB. Graduado em Direito pela UFMG. Procurador Federal de Categoria Especial - AGU. Professor Adjunto da Faculdade de Direito da UFMG e Titular do IBMEC/MG. Ex-Conselheiro da composição original do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPDP), nomeado pela Presidência da República. Fundador e Coordenador da área de concentração em Direito, Tecnologia e Inovação na Pós-Graduação da Faculdade de Direito da UFMG. Fundador e Conselheiro Científico do Centro de Pesquisa em Direito, Tecnologia e Inovação DTIBR (www.dtibr.com). Ex-Membro de Comissões do Conselho Nacional de Justiça, do Conselho da Justiça Federal, da Procuradoria-Geral Federal e da OAB/MG. Pesquisador Visitante na Universidade do Texas em Austin/USA e na Agência de Proteção de Dados do Uruguai. Parceiro tecnológico estratégico na Universidade de Tecnologia de Sydney. Mentor de Equipe no Programa Law Without Walls, LWOW/USA. Citado

em decisões de Tribunais Superiores, por exemplo: STF RE. 1.010.606 e STJ REsp. 1.925.959. Seus textos já foram publicados em mais de 08 países. Áreas de atuação: 1) Direito, Tecnologia e Inovação; 2) Direito Societário; 3) Análise Empírica do Direito (Empirical Legal Studies, ELS). Researcher ID: N-5627-2015. ORCID: 0000-0002-3593-2831. Publicações disponíveis gratuitamente em:
<https://www.researchgate.net/profile/Leonardo-Parentoni>

Equipe de apoio

Fernanda Campos Botelho

Advogada e Mestra em Direito, Tecnologia e Inovação pela Universidade Federal de Minas Gerais. Advogada-sócia da Fernando Botelho Advogados. E-mail: fbotelho@fernandobotelhoadvogados.com.br

Fernanda Sathler Rocha Franco

Doutoranda em Direito na linha interdisciplinar de Tecnologia e Inovação na Universidade Federal de Minas Gerais, mestra em Direito com ênfase em Inovação e bacharela em Ciências Humanas pela Universidade Federal de Juiz de Fora, advogada.

Giovanni Simão Triginelli

Mestrando na Faculdade de Direito da Universidade Federal de Minas Gerais. Graduado em Direito pela Faculdade de Direito da Universidade Federal de Minas Gerais. Advogado.

Laurence Duarte Araújo Pereira

Mestre e Doutorando em Direito pela UFMG. Sócio da Vilar Pereira Paiva e Real Sociedade de Advogados.

Autores

Carolina Adler Cendron

Pós-graduada pelo Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP). Pesquisadora do Laboratório de Governança e Regulação de Inteligência Artificial (Lia.IDP). Advogada no Vieira e Serra Advogados.

Eduardo Serra Rossigneux Vieira

Professor de Direito Empresarial. Sócio Fundador do Vieira e Serra Advogados.

Fernanda Campos Botelho

Advogada e Mestra em Direito, Tecnologia e Inovação pela Universidade Federal de Minas Gerais. Advogada-sócia da Fernando Botelho Advogados. E-mail: fbotelho@fernandobotelhoadvogados.com.br

Fernanda dos Santos Rodrigues Silva

Doutoranda em Direito pela Universidade Federal de Minas Gerais, na área de estudo Direito, Tecnociências e Interdisciplinaridade. Mestre em Direitos na Sociedade em Rede e graduada em Direito pela Universidade Federal de Santa Maria. Coordenadora de Pesquisa e Pesquisadora no Instituto de Referência em Internet e Sociedade (IRIS).

Fernanda Sathler Rocha Franco

Doutoranda em Direito na linha interdisciplinar de Tecnologia e Inovação na Universidade Federal de Minas Gerais, mestra em Direito com ênfase em Inovação e bacharela em Ciências Humanas pela Universidade Federal de Juiz de Fora, advogada.

Gabriella da Silva Reis

Mestra em Direito pela Universidade Federal de Minas Gerais, Especialista em Direito Médico pelo Centro de Ensino Renato Saraiva. Bacharela em Direito pela Universidade Federal do Maranhão. Advogada.

Giovanni Simão Triginelli

Mestrando na Faculdade de Direito da Universidade Federal de Minas Gerais. Graduado em Direito pela Faculdade de Direito da Universidade Federal de Minas Gerais. Advogado.

Helena Penna Marchi

Mestranda em Direito pela UFMG. Advogada.

Henrique Almeida Bazan

Mestre e bacharel em Direito pela Universidade Federal de Minas Gerais

Inma Conde

International Lawyer, Casual Lecturer and PhD Candidate, University of Sydney

Jéssica Fernandes Rocha

Mestre em Direito pela Universidade Federal de Minas Gerais (UFMG). Advogada em Privacidade, Proteção de Dados e Inteligência Artificial. Certified Data Protection Officer in Brazil (CDPO/BR) pela International Association of Privacy Professionals (IAPP). Pesquisadora do Grupo de Estudos em Direito e Tecnologia da Universidade Federal de Minas Gerais (DTEC-UFMG). Membro efetivo da Comissão de Proteção de Dados da OAB/MG. E-mail: jessica.jfr@hotmail.com

José Luiz de Moura Faleiros Júnior

Doutor em Direito pela USP e pela UFMG. Mestre e Bacharel em Direito pela UFU. Advogado. E-mail: josefaleirosjr@outlook.com

Laurence Duarte Araújo Pereira

Mestre e Doutorando em Direito pela UFMG. Sócio da Vilar Pereira Paiva e Real Sociedade de Advogados.

Leonardo Andrade Macedo

Mestre e Doutorando em Direito pela UFMG; Procurador da República.

Lorenzo Antonini Itabaiana

Mestrando em Direito e Tecnologia pela UFMG. Bacharel em Direito pela UFMG. Advogado. E-mail: lorenzoantonini@gmail.com

Maelle Antunes Pereira Lima

Bacharel em Direito pela Faculdade de Direito Milton Campos. Especialista em Direito do

Trabalho pelo CAD. Advogada trabalhista na Sociedade de Advogados Caldeira Brant.

Maria Cláudia Viana Hissa Dias do Vale Gangana

Mestre pela Faculdade de Direito Milton Campos. Doutoranda em Direito pela UFMG. Advogada na Gangana Sociedade de Advogados. Professora do Centro Universitário Estácio de Belo Horizonte.

Natália Cristina Chaves

Mestre e Doutora em Direito Empresarial pela UFMG. Professora da Graduação e do Programa de Pós-Graduação em Direito da UFMG. Sócia fundadora da Passos e Chaves Sociedade de Advogados.

Sumário

PREFÁCIO.....	VII
APOIO INSTITUCIONAL.....	XV
BREVES CURRÍCULOS DOS COORDENADORES E DOS AUTORES.....	XV
SUMÁRIO	XXI

I

ANTECEDENTES DO MARCO CIVIL DA INTERNET

CAPÍTULO 1 DIGITAL CONSTITUTIONALISM IN PRACTICE: THE LEGISLATIVE EVOLUTION OF BRAZIL’S MARCO CIVIL DA INTERNET (2014-2015).....	31

Inma Conde

I. Introduction.....	32
II. Law No. 12,965 of April 23, 2014 (<i>Marco Civil da Internet</i>).....	34
III. Senate Approval and Final Adoption.....	36
IV. Explanatory Memoranda.....	37
V. Relevant Bills (2019–2025).....	37
V.1. Early Legislative Process.....	38
V.2. Legal Validity, Amendments and Legal Interplay in the <i>Marco Civil da Internet</i>	40
V.3. Decree No. 8,771, 11 May 2016.....	42
V.4. Amendments	45
VI. Conclusion	74
References.....	75

II

PERÍCIA FORENSE COMPUTACIONAL

CAPÍTULO 2 MARCO CIVIL DA INTERNET E PROVA DIGITAL: AVANÇOS E LIMITAÇÕES.....	81

Leonardo Andrade Macedo

Sumário

1. Introdução	81
2. Tipos de dados e obtenção de provas digitais nas comunicações pela internet	87
2.1 Dados cadastrais	89
2.2 Dados de tráfego	92
2.3 Dados de conteúdo	95
3. Conservação dos dados nas comunicações pela internet.....	99
3.1 Guarda de dados (<i>data retention</i>).....	100
3.2 Preservação de dados (<i>data preservation</i>)	102
4. Conclusão	106
Referências	107

CAPÍTULO 3 INCIDENTES DE SEGURANÇA COM DADOS PESSOAIS EM SERVIÇOS DE ARMAZENAMENTO EM NUVEM: PRESERVAÇÃO DE EVIDÊNCIAS DIGITAIS E DEVERES DE COMUNICAÇÃO	111

Jessica Fernandes Rocha

Introdução	112
1. Gestão de incidentes de segurança da informação com dados pessoais.....	113
1.1. Conceitos Elementares	114
1.2. Desafios na preservação de evidências digitais	116
1.3. Pontos de atenção na interpretação de evidências digitais.....	119
1.4. Pontos de atenção na preservação de evidências digitais.....	122
2. Cadeia de custódia em provas digitais	126
2.1. O papel da cadeia de custódia na investigação cibernética.....	127
2.2. Um <i>framework</i> baseado na ISO/IEC 27037:2013.....	128
3. Deveres de comunicação em incidentes de segurança com dados pessoais.....	133
3.1. Categorização e comunicação entre agentes de tratamento.....	134
3.2. Comunicação à Autoridade Nacional de Proteção de Dados	135
3.3. Comunicação aos titulares	136
Conclusão	136
Referências	137

III

NEUTRALIDADE DA REDE

CAPÍTULO 4 10 ANOS DO MARCO CIVIL DA INTERNET: BREVES REFLEXÕES SOBRE	

NEUTRALIDADE DA REDE	143
<i>Giovanni Simão Triginelli</i>	

1. Introdução	144
2. Neutralidade de Rede	146
2.1. Breve relato histórico	146
2.2 Análise histórica da neutralidade de rede no Brasil	153
2.3 Exceções à regra da neutralidade de rede	157
3. Conclusão	168
Referências	169

CAPÍTULO 5 OS ASPECTOS ECONÔMICOS DO FAIR SHARE SOB A ÓTICA DA NEUTRALIDADE DA REDE	173
<i>Fernanda Campos Botelho</i>	

Introdução	174
1 O <i>fair share</i>	176
2 Os riscos à neutralidade de rede	178
3 O caso SK Broadband v. Netflix	178
4 O caso Deutsche Telekom v. Meta	181
5 Os debates no Brasil quanto ao tópico	182
6 Previsões e Conclusões	189
Referências	194

IV

PROVEDORES DE SERVIÇO (ISP'S): ESPÉCIES, GUARDA DE REGISTROS E RESPONSABILIDADE CIVIL

CAPÍTULO 6 DEVERES JURÍDICOS DOS PROVEDORES DE INTERNET E GUARDA DE REGISTROS	199
<i>Lorenzzo Antonini Itabaiana, José Luiz de Moura Faleiros Júnior</i>	

Introdução	200
1. Os provedores de Internet e suas classificações	202
1.1. Definição de Serviços de Telecomunicações e Valor Adicionado	203
1.2. <i>Digital Millennium Copyright Act</i> (DMCA)	205

Sumário

1.3. Categorização Infraestrutural (1999).....	206
1.4. Categorização finalística (2001)	207
1.5. Categorização Contextual (2010).....	209
1.6. Tipologia de Provedores de Serviços	210
2. Deveres de guarda de registros e contextos específicos.....	211
3. Endereço IP e portas lógicas	219
3.1. <i>Internet Protocol</i> (IP)	219
3.2. Portas lógicas.....	220
Conclusão	224
Referências	225

CAPÍTULO 7 PROVEDORES DE APLICAÇÃO E CONTEÚDO DE TERCEIROS: UMA ANÁLISE DA EVOLUÇÃO JURISPRUDENCIAL	229

Henrique Almeida Bazan

Introdução	230
1. O conceito de provedores de aplicação	232
2. O regime de responsabilidade civil de provedores de aplicação por conteúdos de terceiros	235
3. Decisões singulares e a evolução jurisprudencial	237
3.1. Provedores de pesquisa	238
3.2. Provedores de mensageria criptografados	242
3.3. Proteção da criança e do adolescente.....	245
4 Considerações finais	248
Referências	249

V

MODERAÇÃO DE CONTEÚDO, LIBERDADE DE EXPRESSÃO E DIREITOS FUNDAMENTAIS

CAPÍTULO 8 <i>SHADOWBANNING</i> : UMA TÉCNICA CONTROVERSA DE MODERAÇÃO DE CONTEÚDO DIGITAL.....	255

Fernanda Sathler Rocha Franco

1. Introdução	257
2. <i>Shadowbanning</i> nas plataformas digitais: forma de moderação de conteúdo, “curadoria” de	

conteúdo ou espécie de sanção imposta ao usuário?	259
2.1 Algumas delimitações conceituais desta prática	260
2.2 <i>Shadowbanning</i> : procedimento e principais aplicações	262
3. Aspectos regulatórios do <i>shadowbanning</i> : observação normativa a partir do <i>Digital Services Act</i> (DSA) e do Marco Civil da Internet.....	265
3.1 Digital Services Act (DSA).....	265
3.2 Marco Civil da Internet (MCI):	269
4. Código Civil, Código de Defesa do Consumidor e Lei Geral de Proteção de Dados como possíveis fundamentos jurídicos para a abordagem do <i>shadowbanning</i> : prós e contras	272
4.1 Código Civil e a teoria do abuso de direito.....	273
4.1.1 <i>Shadowbanning</i> nas plataformas digitais: O caso Marcela Balandez x Facebook	276
4.2 Código de Defesa do Consumidor (CDC): direito de transparência do usuário-consumidor quanto à prática de <i>shadowbanning</i>	278
4.3 Lei n. 13.709/18 (Lei Geral de Proteção de Dados): direito à transparência e direito à revisão de decisões automatizadas sobre a prática de <i>shadowbanning</i>	281
4.4 Projeto de Lei n. 2630/2020 - Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet	288
5. Discussão e conclusão	291
Referências	293

CAPÍTULO 9 MODERAÇÃO AUTOMATIZADA EM REDES SOCIAIS E O NECESSÁRIO DIÁLOGO ENTRE A REGULAÇÃO DE PLATAFORMAS DIGITAIS E A REGULAÇÃO DA INTELIGÊNCIA ARTIFICIAL	299

Fernanda dos Santos Rodrigues Silva

Introdução.....	300
1 O Marco Civil da Internet e a evolução dos desafios da moderação de conteúdo em plataformas digitais.....	301
2 Desafios da moderação de conteúdo por IA e as ameaças a direitos fundamentais em plataformas digitais.....	307
3 As intersecções entre a regulação de plataformas e de inteligência artificial para uma moderação de conteúdo confiável e legítima	316
3.1 Princípios e direitos para usuários de plataformas digitais e pessoas afetadas por sistemas algorítmicos.....	317
3.2 Medidas de governança e transparência para agentes envolvidos com moderação automatizada de conteúdo	321

Sumário

4 Conclusão	325
Referências	327

CAPÍTULO 10 | A (IN)CONSTITUCIONALIDADE DO ART. 19 DO MARCO CIVIL DA INTERNET 333

Natália Cristina Chaves, Helena Penna Marchi

1. Introdução	334
2. O modelo de <i>notice and take down</i>	338
3. O modelo de <i>notice and stay down</i>	344
4. A responsabilidade civil dos provedores de aplicações no Marco Civil da Internet	347
5. O julgamento da matéria pelo Supremo Tribunal Federal	352
5. Conclusão	361
Referências	362

CAPÍTULO 11 | ENTRE A LIBERDADE DE EXPRESSÃO E A CENSURA NA ERA DIGITAL: UMA ANÁLISE DO ARTIGO 19 DO MARCO CIVIL DA INTERNET 367

Eduardo Serra Rossigneux Vieira, Carolina Adler Cendron

1. Introdução	368
2. O Marco Civil da Internet e o artigo 19	370
3. Os desafios e proteções legais do direito fundamental da liberdade de expressão na Internet	376
4. Moderação de conteúdo e responsabilidade dos provedores de aplicação	379
5. Reanálise da constitucionalidade do art. 19 do Marco Civil da Internet pelo Supremo Tribunal Federal: julgamento conjunto dos temas 987 e 533 de repercussão geral	384
6. As possíveis implicações para a liberdade de expressão em caso de ser declarada inconstitucionalidade do art. 19 do MCI	386
7. Conclusão	389
Referências	391

CAPÍTULO 12 | MONITORAMENTO E MODERAÇÃO DE CONTEÚDO MÉDICO NAS REDES SOCIAIS 393

Gabriella da Silva Reis

1. Introdução	394
2 Atuação do Conselho Federal e dos Conselhos Regionais de Medicina	395

3 Contexto da Publicidade e Propaganda Médica no Brasil	397
4 Monitoramento de Conteúdo sobre Saúde pelos Conselhos Regionais de Medicina.....	403
5 Moderação de conteúdo de saúde realizado pela Meta no Instagram	406
5.1 Marco Civil da Internet e Moderação de Conteúdo	406
5.2 Estruturas Organizacionais de Moderação.....	407
5.3 Diretrizes e Políticas da Meta para uso do Instagram	408
5.4 Moderação Automatizada.....	410
6. Convergências e Divergências entre o Papel de Monitoramento dos Conselhos Regionais de Medicina e a Moderação de Conteúdo exercida pela Meta	412
7 Proposta de Governança Colaborativa	414
8 Conclusão	417
Referências	418

VI

REGULAÇÃO DE PLATAFORMAS DIGITAIS: LIBERDADE DE EXPRESSÃO OU EXERCÍCIO DE PODER?

CAPÍTULO 13 REGULAÇÃO DE PLATAFORMAS DIGITAIS: LIBERDADE DE EXPRESSÃO OU EXERCÍCIO DE PODER?	423
<i>Laurence Duarte Araújo Pereira, Maelle Antunes Pereira Lima, Maria Cláudia Viana Hissa Dias do Vale Gangana</i>	

1. Introdução	424
2. Marco civil da internet e regulação das plataformas digitais	427
3. A constitucionalidade do artigo 19 do Marco Civil da Internet à luz dos temas 533 e 987 do Supremo Tribunal Federal	434
4. A discussão da constitucionalidade do artigo 19 do Marco Civil da Internet sob a ótica da liberdade de expressão e os riscos no aumento do exercício de poder pelas plataformas digitais.....	449
5. Conclusão	454
Referências	455

I
ANTECEDENTES DO
MARCO CIVIL DA INTERNET

DIGITAL CONSTITUTIONALISM IN PRACTICE: THE LEGISLATIVE EVOLUTION OF BRAZIL'S MARCO CIVIL DA INTERNET (2014-2015)

Inma Conde

International Lawyer, Casual Lecturer and PhD Candidate, University of Sydney

DOI: <https://doi.org/10.59224/dti7.ch1>

Resumo: Este artigo investiga a trajetória legislativa do *Marco Civil da Internet* (Lei nº 12.965/2014), desde sua origem até suas emendas subsequentes e projetos de lei relacionados, abrangendo o período até 2025. Oferece uma análise abrangente de como a principal lei brasileira sobre governança da internet evoluiu em resposta a novas demandas regulatórias em áreas como proteção de dados, responsabilização de plataformas e discriminação algorítmica. Apesar da centralidade do *Marco Civil* nos debates globais sobre governança da internet, poucos estudos acadêmicos examinaram seu desenvolvimento legislativo completo ou a interação entre seus princípios originais e as reformas regulatórias emergentes. Este trabalho preenche essa lacuna por meio de uma metodologia de historiografia legislativa, examinando sistematicamente leis, decretos, projetos de lei e registros parlamentares oficiais. Apresenta três principais contribuições à literatura existente: primeiro, reconstrói a cronologia legislativa do *Marco Civil* e de seus instrumentos correlatos; segundo, analisa como sua estrutura normativa original incorporou novas obrigações jurídicas sem perder coerência; e terceiro, oferece um modelo conceitual para compreender como leis digitais baseadas em direitos

Abstract: This paper investigates the legislative trajectory of Brazil's *Marco Civil da Internet* (Law No. 12.965/2014) from its inception through its subsequent amendments and related bills up to 2025. It offers a comprehensive analysis of how Brazil's foundational internet law has evolved in response to new regulatory demands in areas such as data protection, platform accountability, and algorithmic discrimination. Despite the centrality of the *Marco Civil* to global internet governance debates, little scholarship has examined its full legislative development or the interplay between its original principles and emerging regulatory reforms. This paper addresses that gap by employing a legislative historiography methodology, systematically examining laws, decrees, bills, and official parliamentary records. It makes three key contributions to existing literature: first, it reconstructs the legislative chronology of the *Marco Civil* and its related instruments; second, it analyses how the original normative structure has absorbed new legal obligations without losing coherence; and third, it provides a conceptual framework for understanding how rights-based digital laws evolve over time. The main conclusion is that the *Marco Civil* has served as a resilient constitutional anchor capable of

evoluem ao longo do tempo. A principal conclusão é que o *Marco Civil* atuou como um pilar constitucional resiliente, capaz de integrar reformas sem comprometer seu caráter democrático e fundamentado em direitos.

Palavras-chave: Constitucionalismo Digital; Marco Civil da Internet; governança da internet; regulação de plataformas; historiografia legislativa; lei de proteção de dados; Brasil.

integrating reforms while maintaining its foundational democratic and rights-based character.

Keywords: Digital constitutionalism; Marco Civil da Internet; internet governance; platform regulation; legislative historiography; data protection law; Brazil.

CONTENTS: I. Introduction; II. Law No. 12,965 of April 23, 2014 (Marco Civil da Internet); III. Early Legislative Process; IV. Legal Validity, Amendments and Legal Interplay; V. Relevant Bills (2019–2025); VI. Conclusion VII. References.

I. INTRODUCTION

This article examines the legislative process of Brazil’s Civil Rights Framework for the Internet—Marco Civil da Internet (Law No. 12.965/2014)—from its inception in 2009 through its enactment in 2014 and subsequent regulatory and legislative developments up to 2025. The Marco Civil represents a foundational statute in Brazil’s digital governance, articulating constitutional principles such as privacy, freedom of expression, and net neutrality within the online environment. Its legislative process was unprecedented in Brazilian legal history, marked by wide public consultation, cross-sector collaboration, and intense congressional debate.

To uncover the law’s normative foundations and institutional evolution, this article draws on a methodology grounded in legislative historiography. It systematically analyses original bills, public consultation records, parliamentary reports, and regulatory instruments. These materials were accessed via the Brazilian Federal Senate’s legislative portal, using a relevance-sorted search for legislative proposals related to Law No. 12.965.¹ The study focuses on nine key bills, spanning from 2019 to

1. Senado Federal (Brazil), *Portal do Senado Federal* (Web Page)

2025, which either amended, interpreted, or sought to reform the Marco Civil. Among the most significant legislative actions are Law No. 13.709/2018 (LGPD), Decree No. 8.771/2016, and proposed reforms such as Bill No. 2922/2020 and Bill No. 2821/2022.

The signing of the Decree on the Brazilian Civil Rights Framework for the Internet (Marco Civil da Internet) was one of the last acts of Dilma Rousseff as President of the country. While the nation watched the final vote on the opening of impeachment proceedings in the Federal Senate, the elected President signed Decree No. 8,771 of 11 May 2016,² which regulates Law No. 12,965 of 23 April 2014, establishing the Marco Civil da Internet (MCI). Its text specifically addresses the permitted instances of data packet discrimination on the internet and traffic degradation, outlines procedures for data retention and protection by connection and application providers, points to transparency measures regarding the public administration's requests for registration data, and establishes parameters for monitoring and investigating violations.³

The objective of this article is to contextualise the Marco Civil's core provisions—such as data protection, intermediary liability, and net neutrality—within the broader legislative ecosystem that shaped them. The article considers a plurality of legislative sources that reveal the dynamic interplay between civil society demands, political negotiations, and global regulatory influences. It highlights how contested concepts were resolved in law, how subsequent legal instruments such as the LGPD reshaped core provisions, and how proposed bills signal Brazil's evolving stance on content regulation, platform accountability, and digital rights.

<https://www6g.senado.leg.br/busca/> accessed 15 February 2025; Senado Federal (Brazil), 'Resultados da Busca: "12.965"' (Web Page) <https://www6g.senado.leg.br/busca/?portal=Atividade+Legislativa&q=12%2C965&p=2> accessed 15 February 2025.

2. *Decreto nº 8.771, de 11 de maio de 2016 (Brazil)*, 'Regulamenta a Lei nº 12.965, de 23 de abril de 2014' (11 May 2016).
3. Maria Alejandra Nicolás et al, 'A Primeira Fase da Consulta Pública da Regulamentação do Marco Civil da Internet: Estrutura Comunicativa, Limites e Contribuições' (2017) 15(2) *contemporanea | comunicação e cultura* 485, 486; Soraia Herrador Costa Lima de Souza, *Internet Policy Framing in Emerging Economies: A Case Study of Marco Civil da Internet, A Brazilian Law for Internet Governance* (Social Science Research Network, 1 December 2016).

What this chapter contributes—and what has thus far been underdeveloped in Brazilian and comparative literature—is a chronological legislative reconstruction of how the *Marco Civil* has been interpreted, expanded, and challenged over time. This approach not only clarifies the internal legal coherence of the framework but also reveals how the *Marco Civil* has acted as a legislative “anchor,” absorbing new governance demands in areas such as data protection, algorithmic discrimination, content moderation, and digital commerce. By aligning statutory amendments (such as the LGPD) and recent legislative proposals with the *Marco Civil*’s foundational principles, the chapter demonstrates how a rights-based internet law can evolve without losing its normative core. By providing a detailed legislative chronology and legal analysis, the article contributes to a better understanding of how digital constitutionalism has been constructed in Brazil. It also serves as a reference for comparative legal scholars and policymakers navigating the challenges of internet regulation in democratic societies.

II. LAW NO. 12,965 OF APRIL 23, 2014 (*MARCO CIVIL DA INTERNET*)

Law No. 12,965 of April 23, 2014,⁴ commonly referred to as the *Marco Civil da Internet*, represents Brazil’s foundational legal framework governing the use of the internet. Enacted by the National Congress and sanctioned by President Dilma Rousseff, the law establishes a comprehensive charter of rights and responsibilities applicable to users, internet service providers, content platforms, and public authorities. It is grounded in constitutional values, notably the protection of privacy, freedom of expression, and access to information.

Article 1 defines the scope of the law, affirming its applicability to all entities operating within the Brazilian digital environment, including foreign service providers that offer services to users located in Brazil. Articles 2 through 4 frame the internet as an essential tool for democratic participation, civic engagement, and the exercise of fundamental rights, underscoring its social function in contemporary society.

Adopting a rights-based regulatory approach, the *Marco Civil* articulates its

4. Lei nº 12.965 de 23 de abril de 2014 (Brazil), ‘Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil’ (24 April 2014) *Diário Oficial da União*.

guiding principles in Article 3. These include the preservation of network functionality, openness, pluralism, freedom of business models, human rights, consumer protection, and free competition. The law explicitly protects internet users through Chapter II (Articles 7 and 8), which codifies a set of fundamental digital rights. These rights include the inviolability and confidentiality of communications, the protection of personal data, the right to prior, informed, and express consent for data processing, and the right to request the permanent deletion of personal data after termination of a service relationship.

Article 7, in particular, reflects a strong alignment with international standards of data protection, requiring that consent for data processing be free, informed, and clearly distinguishable from other contractual terms. Users must also be provided with transparent information about network management practices, including how their data will be handled and for what purposes.

One of the law's central provisions is the enshrinement of net neutrality under Article 9. It prohibits the discrimination or degradation of internet traffic based on content, origin, destination, service, or application. Exceptions are allowed only for essential technical requirements or prioritisation of emergency services, and such exceptions must be transparent, proportionate, and communicated to users in advance. This provision positions Brazil among a small group of jurisdictions that explicitly legislate net neutrality at the statutory level.

Data protection and data retention are further regulated under Articles 10 to 16. The law requires internet connection providers and application providers to store access logs under strict security conditions. Access to these records is permitted only under judicial order, except for basic registration information, which may be disclosed to administrative authorities under specific legal conditions. The law also adopts data minimisation principles, ensuring that providers collect and retain only the data strictly necessary for the provision of services [6].

With respect to intermediary liability, Articles 18 to 21 establish a regime of conditional exemption for internet application providers. These entities are generally not held liable for content generated by third parties unless they fail to comply with a specific court order requiring the removal of infringing material. This safe harbour approach reflects a balance between protecting platforms from overregulation and

ensuring accountability for violations of rights, particularly in cases of defamation or copyright infringement.

Special provisions are made for violations of privacy and dignity, such as the unauthorised disclosure of intimate images. In such cases, providers may be held subsidiarily liable if they do not act expeditiously upon receiving appropriate notification.

Judicial access to personal data and logs is regulated under Articles 22 and 23, which impose stringent safeguards. Requests must be specific and justified within the context of civil or criminal proceedings, and judicial orders must respect confidentiality and the principle of necessity. These safeguards reflect the legislature's intention to prevent abusive or disproportionate use of user data in litigation.

Finally, the law outlines the duties of the State in Articles 24 to 28, which include promoting digital inclusion, ensuring interoperability among public services, enhancing transparency in public data, and supporting the development of national technologies and content. Article 29 specifically addresses the protection of children and adolescents online, mandating the adoption of educational and parental control mechanisms. Article 30 enables judicial enforcement of rights, while Article 31 provides transitional provisions, particularly in relation to copyright liability, which remains governed by separate legal instruments.

Together, these provisions mark a significant advancement in the regulation of the digital sphere. The *Marco Civil da Internet* not only consolidates users' digital rights in Brazil but also introduces a principled framework for internet governance that balances constitutional protections, regulatory coherence, and technological innovation.

III. SENATE APPROVAL AND FINAL ADOPTION

The legislative history reveals contentious discussions around critical provisions, notably net neutrality and intermediary liability.⁵ These debates were influenced

5. Moisés de Oliveira Nazário, 'Entenda o projeto de Marco Civil da Internet' (Web Page, 3 September 2013), https://www12.senado.leg.br/noticias/materias/2013/09/03/entenda-o-projeto-de-marco-civil-da-internet?utm_source=chatgpt.com

heavily by international developments, particularly the European Union's e-Commerce Directive (2000/31/EC) and the U.S. Communications Decency Act of 1996 (Directive 2000/31/EC, OJ L178/1; Communications Decency Act, 47 USC §230).

The Brazilian Senate swiftly approved the bill in April 2014 (PLC 21/2014), following intense plenary discussions but ultimately refraining from major substantive changes. Senators emphasized the broad consensus already reached in the Chamber, recognizing the importance of swiftly enacting legislation to address urgent digital governance issues (Senado Federal, Ata da Sessão Deliberativa, 22 April 2014). The Senate's decision to uphold the text received from the Chamber reinforced the collaborative and consensus-driven nature of the legislative process. The bill was sanctioned by President Dilma Rousseff on 23 April 2014, as Law 12,965/2014, affirming Brazil's leadership in internet governance globally.

IV. EXPLANATORY MEMORANDA

The Exposição de Motivos nº 86/2011, jointly signed by Brazil's Ministries of Justice, Communications, Science and Technology, and Planning, offers invaluable interpretative guidance. It explicitly recognized the Marco Civil as foundational legislation designed to enable subsequent detailed regulations in areas such as personal data protection and cybersecurity (Ministério da Justiça, Exposição de Motivos Interministerial nº 86/2011).

V. RELEVANT BILLS (2019–2025)

The Marco Civil da Internet exemplifies how inclusive consultation and rigorous legislative scrutiny can produce robust, widely accepted legislation. Its legislative history, richly documented through original drafts, congressional records, and explanatory memoranda, continues to guide its interpretation, ensuring the law evolves consistently with its foundational democratic and rights-based principles.

Understanding this legislative history remains essential for interpreting and applying Brazil's internet framework, reinforcing its role as a reference model internationally.

V.1. Early Legislative Process

The legislative development of Brazil's *Marco Civil da Internet* (Law No. 12.965/2014) was unprecedented in the country's legal history due to its participatory methodology and emphasis on multistakeholder engagement. The process formally began in 2009, when the Federal Government—through the Ministry of Justice—launched a public consultation via an online platform to solicit input on the future of internet regulation in Brazil.⁶ This effort was coordinated in partnership with the Centre for Technology and Society at Fundação Getúlio Vargas (CTS-FGV) and drew heavily on the normative framework articulated in the “Principles for the Governance and Use of the Internet” by the Brazilian Internet Steering Committee (CGL.br).⁷

The process involved multiple stages, including public consultations, parliamentary debates, and negotiations between different sectors. The first phase of public consultation, held in 2009-2010, collected over 1,000 contributions from individuals and organisations, demonstrating a significant level of public engagement. However, participation was not without challenges, as the process was criticised for being overly dominated by specialised groups and lacking broader public awareness.⁸

On the basis of these initial contributions, the government introduced Draft Bill No. 2.126/2011 to the Chamber of Deputies in 2011. The bill—soon known as the *Marco Civil da Internet*—represented a rights-based approach to internet regulation, with explicit reference to the Federal Constitution. The bill recognised that internet access is essential to the exercise of citizenship and that its governance must be grounded in the protection of individual rights, including freedom of expression, the inviolability of private communications, and the participatory nature of the

6. Carlos Affonso Pereira de Souza, Fabro Steibel and Ronaldo Lemos, 'Notes on the Creation and Impacts of Brazil's Internet Bill of Rights' (2017) 5(1) *The Theory and Practice of Legislation* 73.

7. Moisés de Oliveira Nazário, 'Entenda o Projeto de Marco Civil da Internet' *Agência Senado* (online, 3 September 2013) <https://www12.senado.leg.br/noticias/materias/2013/09/03/entenda-o-projeto-de-marco-civil-da-internet> accessed 3 March 2025.

8. Samuel Anderson Rocha Barros, 'Os desafios das consultas públicas online: lições do Marco Civil da Internet' (2016) 12(1) *Liinc em Revista* 72; Rachel Callai Bragatto, Rafael Cardoso Sampaio and Maria Alejandra Nicolás, 'Inovadora e democrática. Mas e aí? Uma análise da primeira fase da consulta online sobre o Marco Civil da Internet' (2015) 14(29) *Política & Sociedade* 125.

network.⁹

The draft outlined several objectives, notably the universalisation of internet access and the encouragement of technological innovation. Among the key rights guaranteed were: the inviolability and confidentiality of internet communications, except under judicial order; the right to uninterrupted access, save for non-payment; the assurance of service quality as contracted; transparency in contractual terms; and protection of access and usage data from third-party disclosure without the user's informed consent [5]. In addition, the bill established a conditional liability regime for internet intermediaries: platforms such as YouTube or Facebook would not be held liable for user-generated content unless they failed to comply with a specific court order for its removal.¹⁰

The second phase of consultation, which took place in 2012, was designed to deepen and structure the debate on core issues identified in the first phase. This stage saw a surge in civil society engagement and focused on refining provisions related to data protection, intermediary liability, and particularly net neutrality. Contributions during this phase often reflected libertarian perspectives that called for minimal state intervention and strong guarantees for digital freedoms.¹¹¹²

Parliamentary deliberation intensified thereafter. A Special Committee, chaired by Deputy Alessandro Molon, organised public hearings and debates across various regions of Brazil to gather geographically diverse input. Throughout this process, intense negotiation occurred between civil society, telecommunications companies, and government representatives, especially around contentious topics such as

9. Moisés de Oliveira Nazário, 'Entenda o Projeto de Marco Civil da Internet' *Agência Senado* (online, 3 September 2013) <https://www12.senado.leg.br/noticias/materias/2013/09/03/entenda-o-projeto-de-marco-civil-da-internet> accessed 3 March 2025.

10. Ibid.

11. Rachel Callai Bragatto, Rafael Cardoso Sampaio and Maria Alejandra Nicolás, 'Inovadora e democrática. Mas e aí? Uma análise da primeira fase da consulta online sobre o Marco Civil da Internet' (2015) 14(29) *Política & Sociedade* 125.

12. Raphael Silveiras and Gilda Figueiredo Portugal Gouvea, 'A presença do Estado na rede: Marco Civil da Internet e reforma da Lei de Direito Autoral' (2016) 12(1) *Liinc em Revista* 132.

mandatory local data storage and the scope of liability exemptions.¹³¹⁴ Despite these disagreements, the legislative process maintained its participatory ethos and culminated in the approval of the bill in April 2014. The law was sanctioned by President Dilma Rousseff on 23 April 2014 and came into effect shortly before the *NetMundial Global Multistakeholder Meeting on the Future of Internet Governance*, held in São Paulo. This timing was symbolic, reflecting Brazil's commitment to open, democratic digital governance.¹⁵

V.2. Legal Validity, Amendments and Legal Interplay in the *Marco Civil da Internet*

The Marco Civil da Internet (Law No. 12.965/2014) stands as a foundational statute for internet governance in Brazil, articulating a set of principles, rights, and obligations applicable to users, providers, and public authorities. As a legal framework, it affirms essential guarantees such as net neutrality, data protection, freedom of expression, and privacy in digital environments. Since its enactment, the law has undergone critical interpretative developments, influenced both by attempted reforms and by the incorporation of other legislative instruments—most notably, the Lei Geral de Proteção de Dados (LGPD).

One of the most significant valid amendments to the Marco Civil emerged with the Law No. 13.709/2018 (LGPD), which regulates the processing of personal data. This law introduced important clarifications and substantive modifications to Articles 7 and 16 of the Marco Civil. For instance, Article 7(X) was amended to ensure that the right to delete personal data must comply not only with the Marco Civil but also with the protective conditions set forth in the LGPD. Similarly, Article 16(II) was revised to permit the retention of personal data beyond the original purpose, provided that such retention aligns with the lawful bases and exceptions outlined

13. Guilherme Francisco Waterloo Radomsky and Fabrício Solagna, 'Marco Civil da Internet: Abrindo a Caixa-Preta da Agenda de uma Política Pública' (2016) 12(1) *Liinc em Revista* 154.

14. Laura Vilela Rodrigues Rezende and Meyrielle Rodrigues de Lima, 'Governança Na Internet: Um Estudo Sobre o Marco Civil Brasileiro' (2016) 19(1) 133 <<https://dialnet.unirioja.es/descarga/articulo/6499302.pdf>>.

15. Senado Federal, *Ata da Sessão Deliberativa do PLC 21/2014*, 22 April 2014.

under the LGPD. These modifications reflect a growing convergence between Brazil's general data protection regime and its internet regulation, positioning the Marco Civil as part of a broader legal ecosystem grounded in the constitutional rights to privacy, dignity, and informational self-determination.

In contrast, the attempted reforms introduced by Provisional Measure No. 1.068/2021 were explicitly rejected by the National Congress and thus lack legal force. The provisional measure aimed to recalibrate the regulatory landscape concerning content moderation and user rights on social media platforms. It proposed substantial alterations, including the introduction of new legal definitions for “social networks” and “moderation,” and sought to establish detailed procedures under Articles 8-A to 8-D regarding users' rights to contest content removal and account suspension. It also introduced a new Chapter IV-A on sanctions against platforms that violated the proposed moderation rules. These changes were heavily criticized for curtailing the autonomy of platforms in regulating harmful content and for potentially enabling the spread of misinformation, especially during politically sensitive periods. The rejection of this measure reaffirmed the legislature's commitment to upholding the constitutional principles enshrined in the Marco Civil, such as freedom of expression and due process.

Beyond domestic statutory developments, the Marco Civil was originally drafted with strong influences from the Federal Constitution of 1988, particularly Article 5, which safeguards privacy, intimacy, and freedom of communication. It also engages with other legal instruments, including the Civil Code (Law No. 10.406/2002)—specifically, Article 927 on liability for damages—as well as the Consumer Protection Code (Law No. 8.078/1990) and the Statute of the Child and Adolescent (Law No. 8.069/1990). These cross-references serve not merely as ancillary support but as integral parts of a legal fabric that lends normative consistency to the application of the Marco Civil, especially in the areas of data processing, consumer rights, and child protection.

The law also establishes jurisdictional reach beyond national borders. Article 11 affirms that any internet-related activity involving data processing that occurs within Brazilian territory—or that targets Brazilian users—must comply with Brazilian law, even when the service is provided by a foreign entity. This extraterritorial application is of particular importance for transnational data flows and platform liability.

Notably, this provision was also targeted for revocation by MP No. 1.068/2021, but the proposal was rejected, preserving Brazil's ability to enforce its legal standards against multinational digital service providers.

In terms of enforcement and penalties, the Marco Civil contains a sanctions regime under Article 12 that enables administrative penalties, including warnings, fines of up to 10% of a company's gross revenue, and temporary or permanent suspension of activities. These provisions ensure that violations of data privacy and connection records are met with proportionate regulatory consequences. A parallel sanctions chapter introduced under MP No. 1.068/2021 (Chapter IV-A) was also rejected, meaning the original enforcement mechanisms remain in full effect.

The interpretation clause in Article 6 underscores the law's *sui generis* nature by requiring that legal interpretations consider not only normative principles but also the evolving customs and social functions of the internet. This interpretive approach reflects the drafters' awareness of the need for contextual, technology-sensitive readings that maintain normative coherence while embracing digital innovation.

In conclusion, the Marco Civil da Internet remains a robust, constitutionally anchored legal instrument that has evolved to incorporate principles from Brazil's broader legislative and regulatory framework. While attempts to modify it via Provisional Measure No. 1.068/2021 were ultimately unsuccessful, the law has shown resilience in balancing user rights, regulatory flexibility, and Brazil's sovereignty over digital governance. The integration of the LGPD has further consolidated the Marco Civil's role as a cornerstone in the country's data and internet law, making it a subject of continued relevance in both national and international legal scholarship.¹⁶

V.3. Decree No. 8,771, 11 May 2016

Decree No. 8,771/2016 serves as a critical implementing regulation for Brazil's Internet Bill of Rights (Law No. 12,965/2014).¹⁷ While the Marco Civil establishes

16. *Projeto de Lei nº 3207, de 2023* (Brazil) Senado Federal, https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

17. *Decree No 8.771 of 11 May 2016* (Brazil), 'Regulates Law No 12.965 of 23 April 2014' (11 May 2016) *Diário Oficial da União* 7.

fundamental principles and rights, this decree provides the necessary technical and procedural details to make those rights actionable and enforceable. It reflects the hierarchical structure of Brazilian administrative law, where primary legislation sets out general principles, and decrees clarify their practical application.

One of the central contributions of the decree is the detailed implementation of the network neutrality principle set out in Article 9 of the Marco Civil. The decree specifies the technical criteria under which traffic management may be justified, emphasising that such practices must be essential, proportionate, transparent, and non-discriminatory. It mandates providers to inform users in contracts and through public channels when implementing network management practices that may affect data flow. Additionally, it defines the acceptable scenarios for traffic prioritisation, such as emergency communications, and strictly prohibits commercial arrangements that could undermine the open nature of the internet.

In the area of data protection and privacy, the decree elaborates on the obligations contained in Articles 7, 10, and 11 of the Marco Civil. It establishes rigorous security standards for the handling and storage of personal data and records, requiring the use of encryption, access control, and authentication mechanisms. Furthermore, it regulates the format and retention of user registration data and obliges public authorities to present a legal basis and justification when requesting such data from providers. The decree also introduces annual transparency obligations for administrative bodies, a measure absent from the primary law, thereby enhancing accountability regarding state access to personal information.

Institutionally, the decree assigns regulatory and enforcement responsibilities to specific agencies, such as Anatel, Senacon, and CADE, and clarifies their jurisdiction over issues such as technical compliance, consumer protection, and antitrust enforcement. It also affirms that Brazilian law applies extraterritorially in line with Article 11 of the Marco Civil, ensuring that foreign service providers targeting Brazilian users are equally bound by national data protection and neutrality standards.

While the Marco Civil is broad and principle-driven, the decree's role is to provide operational clarity. It translates legal guarantees into enforceable standards and introduces procedural mechanisms that align the implementation of digital rights with international best practices. In this way, the decree reinforces the normative

aspirations of the Marco Civil by ensuring their technical and institutional viability in the evolving internet landscape.

This Decree main provisions include:

1. Network Neutrality (Chapter II)

- Internet data must be treated equally; discrimination or degradation of traffic is only allowed for technical reasons or prioritising emergency services [Decree No 8.771, Art 4]
- Technical traffic management is permitted only to maintain network stability, security, integrity, or functionality [Art 5, Art 6]
- Emergency communications can be prioritised, but must be non-commercial and related to public safety [Art 8]
- ISPs must disclose to users (in simple language and in contracts/websites) any data discrimination or degradation practices [Art 7]
- Deals that compromise the openness of the internet (e.g. commercial prioritisation) are prohibited [Art 9]
- Commercial offers must respect the unified, plural, and inclusive nature of the internet [Art 10]

2. Protection of Personal Data and Privacy (Chapter III)

- Public authorities must state their legal basis and reason when requesting user registration data [Art 11]
- Providers must disclose if they don't collect the requested data [Art 11(1)]
- Registration data includes name, address, and personal qualifications [Art 11(2)]
- Generic/collective data requests are prohibited [Art 11(3)]
- Annual transparency reports must be published by public authorities regarding data requests [Art 12]
- Providers must follow security standards for access control, authentication, logging, and encryption [Art 13]
- Providers must retain the minimum amount of data necessary, and delete it after use or legal deadlines [Art 13(2)]

- Personal data and processing are defined in line with privacy principles [Art 14]
- Data must be kept in structured and accessible formats [Art 15]
- Providers must publish their adopted security standards clearly and accessibly [Art 16]

3. Transparency & Oversight (Chapter IV)

- Anatel oversees technical aspects of the internet and enforces related infractions [Art 17]
- Senacon is responsible for consumer-related internet violations [Art 18]
- CADE investigates violations of economic competition [Art 19]
- Federal agencies must collaborate and can apply Brazilian law even to foreign entities [Art 20]
- Investigations can be initiated by authorities or at the request of any party [Art 21]
- The decree took effect 30 days after its publication [Art 22]

Decree No. 8,771/2016 is essential for implementing the Marco Civil. It translates the law's high-level principles into enforceable actions. By doing so, it strengthens net neutrality, enhances data protection and privacy, and establishes clear oversight mechanisms. This decree bridges the gap between the Marco Civil's broad legislative framework and the technical requirements needed for effective digital rights protection and governance.

V.4. Amendments¹⁸

A) Law No. 13,709, of 2018 (Validity)¹⁹

The General Data Protection Law (Lei Geral de Proteção de Dados Pessoais,

18. *Lei nº 12.965 de 23 de abril de 2014* (Brazil), 'Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil' (24 April 2014) *Diário Oficial da União* 1, <https://legislacao.presidencia.gov.br/atos/?tipo=LEI&numero=12965&ano=2014&ato=93eUTRE9ENVpWTdb6>

19. *Lei No 13.709, de 14 de agosto de 2018*, https://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm#art65..

LGPD), established by Law No. 13,709 of August 14, 2018, is Brazil's comprehensive framework for personal data protection. It was enacted to unify and enhance various data protection regulations, drawing significant inspiration from the European Union's General Data Protection Regulation (GDPR). The LGPD outlines principles, rights, and obligations concerning the processing of personal data, aiming to safeguard individual privacy and promote transparency in data handling practices.

The LGPD also amends Brazil's Internet Civil Framework (Marco Civil da Internet, Law No. 12,965/2014), a landmark law that sets out general rights and responsibilities for internet users and providers. While the Marco Civil broadly affirms user privacy and net neutrality, it lacked comprehensive rules on data processing. The LGPD fills this regulatory gap by refining concepts and imposing concrete obligations on data controllers and processors, both online and offline. Together, these laws form a complementary legal foundation: the Marco Civil articulates digital rights, while the LGPD operationalizes data protection standards within Brazil's evolving digital and administrative landscape.

Since its inception, the LGPD has undergone amendments to refine its provisions and establish enforcement mechanisms. A notable amendment is Law No. 13,853 of July 8, 2019, which introduced significant changes, including the creation of the National Data Protection Authority (Autoridade Nacional de Proteção de Dados, ANPD). The ANPD is tasked with overseeing and enforcing compliance with the LGPD, providing guidelines, and promoting awareness about data protection. This amendment strengthened the institutional framework necessary for the effective application of the LGPD.

Relation to Law No. 12,965 of April 23, 2014 (Marco Civil da Internet)

The Marco Civil da Internet, established by Law No. 12,965 of April 23, 2014, serves as Brazil's "Internet Bill of Rights." It sets out principles, rights, and duties for internet users and service providers, emphasizing freedom of expression, privacy, and net neutrality. While the Marco Civil addresses broader internet governance and user rights, it also contains provisions related to the protection of personal data in the online environment.

The LGPD complements and builds upon the foundations laid by the Marco Civil by providing detailed regulations specifically focused on personal data protection across all sectors, not limited to the internet. In fact, the LGPD explicitly amends certain aspects of the Marco Civil to align Brazil's legal framework with comprehensive data protection standards. For instance, the LGPD enhances definitions and obligations concerning the processing of personal data, thereby extending and specifying the general principles outlined in the Marco Civil.

B) Law No. 13,853 of 2019²⁰

The enactment of Law No. 13.853/2019, which amends the General Personal Data Protection Law (LGPD), represents a decisive step in consolidating Brazil's normative framework for digital rights, data governance, and informational privacy. These developments have directly influenced the interpretation and application of Law No. 12.965/2014, commonly known as the *Marco Civil da Internet*, which initially laid the foundational legal principles for internet regulation in Brazil. While the *Marco Civil* established essential guarantees related to net neutrality, user privacy, and data processing obligations, the amendments introduced by Law No. 13.853/2019 significantly broadened the scope and enforceability of these protections by operationalizing key concepts through a more granular data protection regime.

One of the most consequential legal interactions between these two laws concerns the articulation of user rights and data processing obligations. Under Article 7 of the *Marco Civil*, users have the right to the deletion of personal data once the contractual relationship with a digital service ends. However, Law No. 13.853/2019, through its revision of the LGPD, reinforces this provision by conditioning such deletion on the lawful grounds and legitimate interests described in the LGPD. For instance, Article 16(II) of the *Marco Civil* was revised to align with the LGPD's provisions allowing for the retention of personal data when necessary for compliance with legal obligations or other lawful bases. Thus, the *Marco Civil*'s privacy protections have been effectively strengthened by the LGPD amendments, enhancing legal clarity and

20. Lei No 13.853, de 8 July of 2019, https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm#art1

coherence.

Additionally, Law No. 13.853/2019's establishment of the Autoridade Nacional de Proteção de Dados (ANPD)—a national data protection authority—created a new institutional architecture for overseeing and enforcing data rights in Brazil. Although the *Marco Civil* previously lacked an enforcement body with exclusive competence over data matters, the ANPD now fills that void, with a clearly defined mandate that includes issuing guidelines, applying sanctions, and conducting audits. Articles 55-A through 55-K of the LGPD, introduced by Law No. 13.853/2019, detail the ANPD's regulatory, investigative, and adjudicative functions, thereby institutionalizing the principles previously stated in the *Marco Civil* and providing concrete enforcement mechanisms.

Furthermore, the concept of data portability—recognized in Article 18 of the LGPD—was reinforced in the *Marco Civil* by these amendments, ensuring that individuals can transfer their personal data between service providers. This right is central to user autonomy and is closely aligned with the open and participatory ethos that underpins the *Marco Civil*. By enabling interoperability and consumer choice, the LGPD and its amendments support the broader digital citizenship objectives articulated in Articles 3 and 4 of the *Marco Civil*.

The influence of Law No. 13.853/2019 is also evident in the sanctions regime. While the *Marco Civil* provided for administrative penalties such as fines and suspension of services for non-compliance with data obligations (Article 12), the LGPD amendments expanded the range and specificity of available sanctions. The newly promulgated provisions under Article 52 of the LGPD—including partial database suspension and prohibition of data processing activities—are applicable not only to private actors but also to public entities, provided that procedural safeguards are met. This institutional parity reflects a unified approach to data governance across sectors and strengthens the normative weight of the *Marco Civil*'s original data protection ethos.

In conclusion, Law No. 13.853/2019, by transforming the LGPD and establishing the ANPD, has substantially influenced the *Marco Civil da Internet*, both substantively and institutionally. It has elevated the protections initially envisioned in the *Marco Civil* by introducing enforceable mechanisms, more defined concepts, and

harmonized procedures aligned with global data protection standards. This legal synergy has advanced Brazil's trajectory toward a comprehensive, rights-based model of digital governance, integrating civil liberties, consumer protection, and regulatory accountability in the digital age.

Together, Laws No. 13,709 and 13,853 have transformed the Marco Civil into a more robust and enforceable legal framework. By aligning its provisions with the LGPD's detailed standards and establishing the ANPD's oversight role, these amendments have created a legal regime that is both comprehensive and coherent. They enhance the Marco Civil's privacy and data protection principles, integrate it more firmly into Brazil's broader regulatory landscape, and reinforce its relevance in a global context.

C) Provisional Measure No. 1,068, of 2021²¹ (Rejected)

The Exposição de Motivos Interministerial (EMI) nº 00072/2021, dated 6 September 2021, sets out the justification for Provisional Measure (Medida Provisória) No. 1,068/2021, which sought to significantly amend Law No. 12,965/2014 (Marco Civil da Internet). The stated purpose of the proposed measure was to introduce explicit protections for users of social media platforms, particularly concerning content moderation practices. The document was signed by Ministers Gilson Machado (Tourism), Marcos Pontes (Science, Technology and Innovation), and Anderson Torres (Justice and Public Security), and addressed to the President of the Republic.

The EMI argues that although the Marco Civil da Internet already enshrines principles such as freedom of expression, privacy, and access to information (see *Law No. 12,965/2014, Articles 2–3*), these guarantees were formulated in general terms and were, in the government's view, insufficient to prevent arbitrary moderation of content by social media providers. The measure responds to increasing complaints about users being banned or content being removed without due process, including the absence of clear justification or an avenue for appeal.

To address this, the Provisional Measure proposed adding specific provisions to

21. Medida Provisória nº 1.068, de 6 de setembro de 2021, https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2021/Mpv/mpv1068.htm#art1

the Marco Civil that would:

1. Require just cause and proper motivation for the suspension or removal of accounts, content, or features by social media platforms;
2. Guarantee users the right to *contraditório* (*audi alteram partem*), broad defense, and access to an appeal process;
3. Oblige providers to notify users when taking moderation decisions, with clear information on the measure adopted, the reason for the decision, and the procedures available for contestation;
4. Require platforms to restore content when moderation violates users' rights;
5. Amend the Copyright Law (Law No. 9,610/1998) to allow copyright holders to request administrative sanctions and content reinstatement in cases where moderation violated the user's legal guarantees.

The EMI underscores that these measures were motivated by the perceived mass violation of fundamental rights, especially freedom of expression and due process, exacerbated during the COVID-19 pandemic when social media platforms became primary venues for public discourse.

D) Legal and Political Impact

The Provisional Measure No. 1,068/2021, resulting from this EMI, effectively sought to create a regulatory regime for social media moderation, superimposing detailed due process obligations on private platforms. These included obligations similar to those imposed on state actors, such as procedural fairness, transparent reasoning, and accountability mechanisms for decisions affecting users' rights.

However, the measure was widely criticised by civil society, academia, and digital rights groups for potentially undermining platform autonomy, facilitating the spread of disinformation by limiting moderation capacity, and introducing a chilling effect on content control mechanisms. Critics argued it was a politically motivated intervention ahead of the 2022 election cycle.

Subsequently, the Provisional Measure No. 1,068/2021 was rejected by the President of the Senate on 14 September 2021, just days after its issuance, due to lack of urgency and constitutional concerns. As a result, the amendments proposed through

the EMI were never incorporated into the Marco Civil da Internet. Nonetheless, the episode brought significant attention to the tensions between freedom of expression and content moderation, and sparked ongoing debate over the role of platforms in democratic discourse.

In sum, EMI nº 00072/2021 reflects a legislative attempt to shift the interpretation and application of the Marco Civil towards greater formal control of private moderation practices. Although ultimately unsuccessful, it highlighted the growing regulatory interest in social media governance and laid the groundwork for future legislative proposals seeking to balance platform responsibilities with user rights in Brazil's digital legal landscape.

V.5. Relevant Bills (from 2019 to 2025)²²

A. Bill No. 4807, 2019

- Overview and Legislative Background

Bill No. 4807 of 2019, authored by Senator Soraya Thronicke (PSL/MS), seeks to enhance transparency and accountability in Brazil's digital consumer marketplace by addressing misleading advertising practices in e-commerce. The bill introduces amendments to the Consumer Protection Code (Law No. 8,078/1990), with the express objective of mandating disclosure when products offered online are not physically located within Brazilian national territory at the time of the offer. The legislative proposal responds directly to the proliferation of transnational digital transactions, particularly those involving platforms such as Facebook, Instagram, and other online marketplaces where consumers often unknowingly purchase goods from abroad. Such transactions frequently lead to delayed deliveries, unexpected import charges, or failures in fulfilment due to the lack of adequate information at the point of sale.

22. The methodology of this paper involves a systematic review of relevant bills related to Brazil's Marco Civil da Internet (Law No. 12.965/2014) by utilizing the Brazilian Senate's legislative activity webpage. First, I searched for the law number "12965" within the website's search function. Then, I sorted the results by relevance to ensure that the most pertinent bills were identified. This approach enables a focused selection of bills that align closely with the key principles of the Marco Civil da Internet, ensuring a comprehensive analysis of legislative proposals that may influence the law's application and development.

The bill arises within a broader legislative context in which Brazilian law is adapting to the realities of digital platformisation and cross-border commerce. It reflects growing political concern over the asymmetries of information that place consumers at a disadvantage in online environments, where geographic and legal distances hinder effective redress and undermine confidence in the digital economy.

- Status and Legislative Process

Introduced on 27 August 2019, the bill was referred to the Commission for Transparency, Governance, Oversight and Consumer Protection (CTFC) for substantive examination. As of 2 February 2023, it remains pending within the CTFC and has yet to advance due to the absence of an appointed rapporteur. The bill is therefore in a preliminary stage of legislative scrutiny, awaiting deliberation and committee approval before it may proceed to plenary debate and voting in the Federal Senate.

- Provisions and Legislative Innovations

The bill introduces two substantive legal amendments to the Consumer Protection Code. First, it proposes the addition of a requirement that suppliers operating in online marketplaces must clearly and prominently disclose all essential offer conditions. These include, *inter alia*, the terms of payment, delivery timelines, product availability, and crucially, whether the product is not located in Brazil at the time of the offer. The omission of such information is to be deemed deceptive advertising under Article 37, paragraph 3 of the CDC, which prohibits omissions capable of misleading the consumer about essential characteristics of the product or service.

Second, the bill sets out the legal consequences of non-compliance through the application of existing administrative sanctions available under the CDC. These include monetary fines, the temporary suspension or cancellation of business licenses, and the requirement to issue corrective advertising. The proposed changes clarify that suppliers engaging in cross-border e-commerce shall be treated as “suppliers” for the purpose of these liabilities, thereby ensuring that foreign-based actors operating within Brazilian digital markets are held to the same standards as domestic vendors.

The bill thus offers a novel response to the regulatory challenges posed by

transnational e-commerce. It aims to reduce ambiguity in online transactions by aligning the obligations of digital suppliers with the traditional transparency standards of consumer protection law. This innovation is particularly significant given the proliferation of informal or unverified vendors on social media platforms who frequently obscure the origin and logistics of their goods.

- Relation to the Marco Civil da Internet

While the bill does not propose a direct amendment to the Marco Civil da Internet (Law No. 12,965/2014), it is framed within its normative ecosystem. Article 2(V) of the Marco Civil enshrines consumer protection as a guiding principle of Brazilian internet governance, and Article 7(XIII) explicitly guarantees internet users the right to the application of consumer protection norms in digital commerce. Bill No. 4807/2019 operationalises these provisions by introducing concrete disclosure obligations that target the emerging risks of transnational online retail.

In this sense, the bill is best understood as a legislative complement to the Marco Civil, extending its rights-based framework into the field of commercial regulation. It reflects a convergence of public and private law principles, whereby civil internet rights are interpreted in light of evolving consumer dynamics. Importantly, the bill also reinforces the notion that digital rights are not limited to privacy or expression but must include transparency and informational integrity in commercial relations.

- Potential Legal and Social Impact

If enacted, Bill No. 4807/2019 would significantly enhance transparency and accountability within Brazil's digital economy. By compelling suppliers to disclose the geographic location of goods, the bill provides consumers with the necessary information to make informed decisions and avoid unintended consequences arising from cross-border transactions. It would reduce the incidence of disputes related to shipping delays, hidden fees, and delivery failures—issues that disproportionately affect low-income and first-time digital consumers.

The bill would also contribute to the formalisation and professionalisation of online commerce, encouraging social media vendors and digital platforms to adopt compliance mechanisms consistent with consumer protection law. From a

regulatory standpoint, the measure exemplifies the harmonisation of internet governance with sector-specific legal instruments, thereby reinforcing Brazil's international reputation as a jurisdiction committed to responsible digital regulation.

Furthermore, the proposed amendments carry normative weight. They affirm that the expansion of global e-commerce must not come at the expense of local consumer rights, and that market participation in digital environments must be conditioned by transparency, fairness, and accountability. The bill therefore plays a pivotal role in bridging gaps between internet law and consumer protection, and in adapting the national legal order to the realities of platform capitalism.

In conclusion, Bill No. 4807/2019 offers a pragmatic and principled legal response to the regulatory void in Brazil's cross-border e-commerce landscape. It builds upon the foundational values of the Marco Civil da Internet while introducing precise obligations tailored to the digital economy, thereby reinforcing the legal architecture required for a transparent and equitable online marketplace.

B. Bill No. 2922, 2020²³

- Overview and Legislative Background

Bill No. 2922 of 2020, introduced by Senator Fabiano Contarato (REDE/ES), represents a notable attempt to recalibrate Brazil's digital legal framework by targeting the financial mechanisms that sustain disinformation and hate speech online. The bill seeks to amend Law No. 12,965/2014 (Marco Civil da Internet) by inserting a new provision—Article 19-A—prohibiting both national and foreign companies offering programmatic advertising services from placing advertisements on internet pages identified as disseminating false or hateful content. The legislative motivation stems from growing recognition of the economic infrastructure underpinning the virality of harmful online speech, particularly where automated advertising technologies incentivize the creation and circulation of polarizing, misleading, or violent content.

23. Bill No. 2922, 2020 (Brazil), <https://www25.senado.leg.br/web/atividade/materias/-/materia/142129>

- Status and Legislative Process

As of April 2025, the bill remains pending before the Communication and Digital Law Commission (CCDD) of the Federal Senate. Since 27 August 2024, it has been under the rapporteurship of Senator Esperidião Amin and has yet to proceed to plenary debate. The bill is part of a broader normative shift observed in both national and comparative legal systems, where financial regulation is increasingly seen as a tool for mitigating systemic risks in the digital public sphere. Senator Contarato, a leading proponent of civil rights, environmental integrity, and digital transparency, has framed this initiative as essential for preserving democratic values in the age of algorithmically amplified misinformation.

- Provisions and Legislative Innovations

The central innovation of Bill No. 2922/2020 lies in its insertion of Article 19-A into the Marco Civil da Internet. This article would impose a legal prohibition on the placement of advertisements—via programmatic media services—on websites or digital platforms that are found to promote either verified disinformation or hate speech. Unlike traditional content moderation approaches, this mechanism does not directly address the legality of the content itself but instead interrupts the economic incentives that make such content profitable. The bill draws on comparative models such as the European Union’s Code of Practice on Disinformation, which guides its definitions of “disinformation” and “hate speech.” The latter is further grounded in well-established constitutional jurisprudence concerning incitement to violence or discrimination based on identity markers such as race, ethnicity, religion, gender, or sexual orientation.

In terms of enforcement, the bill empowers regulatory authorities to issue formal warnings and to levy administrative fines of up to 10 percent of the total value of the non-compliant advertising placement. These sanctions are notable not only for their potential scale but also for their scope, as they are applicable to advertising intermediaries, including ad networks and digital platforms. This regulatory focus on intermediaries departs from conventional liability regimes that centre primarily on content producers or hosts, and instead holds accountable those entities that enable the

monetization of harmful material.

- Relation to the Marco Civil da Internet

The proposed amendment marks a substantial departure from the foundational liability regime enshrined in the Marco Civil da Internet. Articles 3 and 19 of the existing law affirm freedom of expression, platform neutrality, and a limited liability model, under which intermediaries are not held accountable for third-party content unless they fail to comply with a specific court order. In contrast, Bill No. 2922/2020 introduces an affirmative duty of care for advertising intermediaries, predicated on their role in sustaining online ecosystems of misinformation. Rather than focusing on the legality of user-generated content per se, the bill reflects a broader turn toward economic accountability, requiring companies to assess and mitigate the advertising-related risks associated with platform monetization. This shift is emblematic of a post-2018 evolution in global internet governance, which increasingly views financial structures—not just legal speech doctrines—as critical levers for addressing online harm.

- Potential Legal and Social Impact

Should it be enacted, Bill No. 2922/2020 would introduce a novel form of intermediary liability into Brazilian internet law, targeting the programmatic advertising infrastructure that underwrites the proliferation of harmful digital content. The bill's regulatory strategy—economic disincentivization—has the potential to dislodge the financial logic that fuels the production and circulation of disinformation and hate speech. In doing so, it may enhance transparency and accountability in the digital advertising market while reinforcing constitutional commitments to dignity, pluralism, and the integrity of democratic discourse.

From a doctrinal perspective, the bill could catalyse significant jurisprudential debates concerning the boundaries of commercial freedom, the scope of intermediary responsibility, and the permissible limitations on platform-based economic activities. By holding advertising networks and platforms accountable for the environments in which their ads appear, the law introduces a differentiated liability framework that moves beyond user-centric notions of rights and instead focuses on the

structural conditions that shape online speech and access to information. Furthermore, the proposed regime may serve as a comparative reference point for jurisdictions exploring non-censorship-based approaches to disinformation control. In linking platform responsibility to financial gain, Brazil would position itself at the forefront of an emerging global movement toward normative alignment between economic activity and digital public ethics.

Ultimately, Bill No. 2922/2020 represents a paradigmatic shift in Brazilian digital regulation: from the reactive enforcement of content takedown orders to the proactive deterrence of monetized misinformation. It supplements the foundational values of the Marco Civil da Internet by operationalising them through mechanisms of financial accountability and economic restraint, offering a structural complement to Brazil's ongoing efforts to balance digital freedoms with democratic resilience.

C. Bill 2184, 2022²⁴

- Overview and Legislative Background

Bill No. 2184 of 2022, authored by Senator Telmário Mota (PROS/RR), proposes amendments to Brazil's Marco Civil da Internet (Law No. 12,965/2014), with the objective of strengthening platform obligations to address harmful content online. The legislative initiative responds to the growing concern over digital environments that expose users—particularly children and adolescents—to content inciting physical or psychological harm. The bill explicitly targets platforms that host, disseminate, or fail to address materials that induce, instigate, or coerce individuals into actions posing a risk to their safety or well-being. This initiative reflects a broader societal and regulatory shift toward prioritising user protection over the more traditionally dominant principle of intermediary neutrality. It recognises that the structure of digital communication, especially on social media platforms, facilitates the rapid spread of dangerous content and calls for a more proactive regulatory posture.

- Status and Legislative Process

24. Bill No. 2184, 2022 (Brazil), <https://www25.senado.leg.br/web/atividade/materias/-/materia/154315>

The bill was officially read in the Senate on 9 August 2022 and initially assigned to the Committee on Science, Technology, Innovation and Information Technology (CCT). However, following Resolution No. 14 of 2023, the matter was reassigned to the Communication and Digital Law Commission (CCDD), which is now responsible for its analysis. As of April 2025, the bill remains pending within the CCDD and is currently under the rapporteurship of Senator Zenaide Maia. It has been designated “Matter with the Report,” but has not advanced to plenary discussion or voting. The last recorded legislative update, dated 29 October 2024, indicates that deliberations remain ongoing and that the bill is still in the early stages of the Senate legislative process.

- Provisions and Legislative Innovations

The bill introduces two key modifications to the Marco Civil da Internet. First, it expands the scope of Article 21 to include not only content that violates sexual privacy—already addressed under the existing legal framework—but also content that induces, instigates, or coerces users to inflict harm upon themselves or others, whether physically or psychologically. This amendment extends platform liability by establishing a standard of “diligent” response: failure to act upon notice of such content may trigger subsidiary liability for providers. Second, the bill introduces a new Article 23-A, which imposes proactive duties on social media platforms. Under this provision, platforms must deploy technological tools capable of detecting and blocking access to the specified harmful content before receiving a formal complaint or notification, provided such preemptive action is technologically feasible. The combined effect of these amendments is to shift the existing legal regime away from a purely reactive liability model toward one characterised by affirmative monitoring and prevention obligations.

- Relation to the Marco Civil da Internet

The Marco Civil da Internet, in its original conception, embodies a cautious approach to platform liability, affirming freedom of expression, net neutrality, and privacy as cornerstones of Brazilian digital regulation. Article 19 of the law, in particular, establishes that providers are not liable for third-party content unless they fail to

comply with a court order. The present bill challenges and expands this model by mandating liability in cases where platforms do not act “diligently” upon extrajudicial notice and by introducing, through Article 23-A, a duty of prior detection. This represents a significant reconfiguration of the Marco Civil’s core balance between safeguarding digital freedoms and addressing harms. It reflects an evolving recognition that the traditional intermediary safe harbour may be insufficient in cases involving vulnerable users or where the harm results from inaction in the face of egregious threats to public health and safety. While not entirely repudiating the principle of limited liability, the bill marks a definitive shift toward a duty-of-care framework, particularly in high-risk digital environments.

- Potential Legal and Social Impact

If enacted, Bill No. 2184 of 2022 would mark a notable evolution in Brazilian platform regulation, bringing with it considerable legal and social consequences. It would compel internet application providers, especially social media companies, to invest in content moderation technologies and human oversight systems capable of meeting the new standards of diligence and preemptive detection. This could place a disproportionate burden on smaller platforms, raising questions about regulatory asymmetry and the potential chilling effects on market entry. At the same time, the bill promises substantial benefits in protecting users—particularly minors and psychologically vulnerable individuals—from exposure to manipulative or coercive digital content. It would further solidify Brazil’s emerging role as a jurisdiction at the forefront of regulatory experimentation in platform governance, aligning in part with international trends such as the European Union’s Digital Services Act. However, the introduction of ambiguous concepts such as “psychological coercion” and the requirement of pre-notice removal may also generate constitutional and jurisprudential debates regarding proportionality, due process, and freedom of expression. To mitigate risks of overreach and arbitrary enforcement, any future implementation would need to be accompanied by clear regulatory guidance and judicial oversight mechanisms.

- Overview and Legislative Background

Bill No. 2821 of 2022, introduced by Senator Fabiano Contarato (PT/ES) and filed on 21 November 2022 in the Plenary of the Federal Senate, emerged in response to growing concern about the systemic spread of hate speech, discrimination, and prejudice across social networks and search platforms in Brazil. The proposal addresses the disproportionate harm faced by vulnerable groups—such as those targeted on the basis of race, gender, disability, religion, sexual orientation, and nationality—and seeks to reform Brazil’s digital governance architecture to respond more effectively to structural inequalities reproduced online.

In its justification, the bill identifies key normative tensions in the existing framework of the Marco Civil da Internet (Law No. 12.965/2014), particularly its strong emphasis on freedom of expression and platform immunity. While the Marco Civil sought to protect fundamental user rights in the digital environment, it has inadvertently allowed online intermediaries to operate with minimal obligations regarding harmful or discriminatory content. The bill argues that content moderation powers already available to platforms under their terms of use must be exercised to mitigate social harms. The use of these powers, according to the drafters, does not infringe upon constitutionally protected speech, but rather preserves the democratic and pluralistic character of the internet.

A notable feature of the proposal is its concern with algorithmic bias. The bill contends that the automated systems which govern online interactions can replicate or amplify pre-existing social prejudices, thereby reinforcing discrimination through invisible, unaccountable mechanisms. Accordingly, the proposal advocates for embedding proactive duties into law that require platforms to identify, mitigate, and report algorithmic harms as a matter of regulatory compliance and democratic obligation.

25. Projeto de Lei nº 2821/2022 (Brazil), Senado Federal, 21 November 2022, https://www25.senado.leg.br/web/atividade/materias/-/materia/155169#tramitacao_10358709.

- Status and Legislative Process

As of May 2023, the bill remained under consideration by the Committee on Constitution, Justice, and Citizenship (CCJ), where it awaited the appointment of a rapporteur. Although no amendments were submitted before the statutory deadline, the bill continues to progress under a conclusive decision model. Its anticipated referral to the Committee on Science, Technology, and Innovation (CCT) signals its dual character as both a constitutional rights initiative and a regulatory reform concerned with platform technologies.

- Provisions and Legislative Innovations

Bill No. 2821/2022 introduces three substantive articles—Articles 18-A, 18-B, and 18-C—and amends Article 3 of the Marco Civil da Internet to add “protection from algorithmic discrimination” as a foundational principle. The proposed amendments construct a legal framework grounded in proactive platform accountability and algorithmic transparency.

Article 18-A establishes a duty for internet application providers to implement mechanisms aimed at identifying and minimizing algorithmic bias. These mechanisms must target patterns of automated decision-making that could lead to discriminatory behavior or structural inequality in the online environment. Article 18-B extends this regulatory burden to search platforms, requiring them to filter and suppress results that incite or perpetuate hate, prejudice, or discrimination. Article 18-C is directed at social media platforms and sets forth obligations to create accessible reporting systems for harmful content, to adopt transparent content moderation standards, and to publish regular reports evaluating the efficacy of these systems.

These provisions shift the liability model of the Marco Civil away from a purely reactive system—where liability is triggered only upon judicial notification—to a forward-looking structure premised on prevention, procedural transparency, and user accountability. By doing so, the bill advances a rights-based framework for online equality and elevates digital governance into a space of normative engagement with anti-discrimination law.

- Relation to the Marco Civil da Internet

The legislative innovations in Bill No. 2821/2022 represent a substantive evolution of the principles articulated in the Marco Civil da Internet. The original law, enacted in 2014, enshrined user rights such as net neutrality, privacy, and freedom of expression, and adopted a narrow model of intermediary liability, most notably in Article 19. This model protected platforms from responsibility for third-party content unless a court order was ignored. While this approach was central to the protection of digital civil liberties at the time, the current regulatory environment demands more nuanced tools to confront the harms emerging from automated systems and large-scale content dissemination.

By amending Article 3 to include algorithmic discrimination as a fundamental concern, and by introducing affirmative obligations on platforms under Articles 18-A to 18-C, the bill embeds a new balance into the Marco Civil—one that recalibrates user rights in light of platform responsibilities. It shifts the interpretive frame of the law from one premised solely on the passive protection of users toward an interactive regime that anticipates the harms posed by algorithmic design, content curation, and digital amplification.

- Potential Legal and Social Impact

If enacted, Bill No. 2821/2022 would introduce a significant normative inflection in Brazil's approach to internet regulation. Its legal consequences would be far-reaching, both operationally and doctrinally. It would require digital platforms to adopt and publicize tools capable of detecting algorithmic bias, to actively suppress discriminatory content, and to engage in periodic disclosure through transparency reports. These mechanisms would serve not only as legal compliance tools but also as instruments of democratic accountability.

At the social level, the bill responds directly to longstanding critiques of digital inequality and content-based harms disproportionately affecting marginalized communities. By foregrounding structural bias and algorithmic injustice, it offers a corrective to earlier models of platform neutrality that failed to account for the disparate impact of content amplification. The bill also positions Brazil as a jurisdiction willing to legislate in alignment with international soft law standards, including the United Nations Guiding Principles on Business and Human Rights and the OECD's

frameworks for algorithmic accountability and fairness.

In this respect, Bill No. 2821/2022 transcends a reactive legislative posture and articulates a forward-thinking model of digital rights governance. It reconfigures the Brazilian internet governance framework to accommodate a more inclusive vision of constitutional equality and technological responsibility—one that centers the rights of the digitally vulnerable while preserving the foundational values of openness and pluralism in the online sphere.²⁶

E. Bill No 3207 of 2023²⁷

- Overview and Legislative Background

Bill No. 3207 of 2023, authored by Senator Cleitinho (REPUBLICANOS/MG), proposes an amendment to the Marco Civil da Internet (Law No. 12.965/2014) aimed at prohibiting the offering of mobile internet plans with limited data allowances, commonly referred to as “data caps.” The bill was introduced in response to the increasing reliance of Brazilian citizens on mobile internet as their primary or sole means of digital connectivity, particularly among lower-income populations. According to its justification, the widespread offering of data-capped mobile plans—endorsed by the National Telecommunications Agency (ANATEL)—has generated significant social and economic inequalities by limiting users' ability to fully access and engage with the digital environment. The proposal seeks to address these inequalities by incorporating an express legal guarantee of unrestricted mobile internet access into Article 7 of the Marco Civil da Internet, which enumerates the fundamental rights of users in Brazil's digital sphere.

- Status and Legislative Process

As of April 2025, Bill No. 3207/2023 remains under review in the Senate's

26. Projeto de Lei nº 2821/2022 (Brazil), Senado Federal, 21 November 2022, https://www25.senado.leg.br/web/atividade/materias/-/materia/155169#tramitacao_10358709.

27. Senado Federal, Projeto de Lei nº 3207, de 2023: Altera a Lei nº 12.965, de 23 de abril de 2014, para vedar a oferta de pacotes com franquias limitadas de dados móveis (21 June 2023), <https://www25.senado.leg.br/web/atividade/materias/-/materia/158369>

Committee on Science, Technology, and Innovation (CCT). It is currently awaiting the appointment of a rapporteur and has not yet progressed to deliberation or voting stages. The bill's initial referral to the CCT reflects its dual character as both a consumer rights measure and a structural intervention in the regulation of telecommunications services. While its formal advancement remains pending, the proposal has already prompted public debate concerning the appropriate balance between market regulation and constitutional principles of digital inclusion.

- Provisions and Legislative Innovations

The core innovation of Bill No. 3207/2023 lies in the inclusion of a new paragraph under Article 7 of the Marco Civil da Internet, explicitly prohibiting the commercialization of mobile internet packages that impose usage limits. The provision is designed to guarantee continuous, unrestricted access to mobile internet services, thereby extending the existing guarantees under Article 7 relating to privacy, service quality, and data protection. The proposed text does not merely address technical service standards, but instead frames mobile data access as a matter of substantive rights protection. In doing so, the bill challenges the prevailing contractual model in telecommunications law by imposing a statutory floor below which service providers may not operate. The language of the proposal is rights-affirming in nature, seeking to transform mobile internet from a commodified service into a legally protected instrument of access to information, education, and democratic participation.

- Relation to the Marco Civil da Internet

The proposed amendment fits coherently within the structure and normative goals of the Marco Civil da Internet. Article 7 of the Marco Civil guarantees the inviolability of privacy, the preservation of data confidentiality, and the assurance of service quality and continuity. Bill No. 3207/2023 reinforces these guarantees by adding the requirement that mobile internet services be provided without artificial limitations on data usage. In doing so, it continues the legislative trend of treating internet access not merely as a commercial offering but as a necessary precondition for the exercise of constitutionally enshrined rights, including freedom of expression and access to public services. Importantly, the bill does not alter the general liability

regime established by the Marco Civil but extends its user-rights framework to ensure that digital connectivity is meaningful, equitable, and uninterrupted. This reflects a maturation of the Marco Civil's normative ambitions, aligning its practical implementation with evolving conceptions of digital citizenship and information justice.

- Potential Legal and Social Impact

If enacted, Bill No. 3207/2023 would constitute a significant development in Brazilian internet law by outlawing the imposition of data caps on mobile internet plans. This would mark a shift from consumer-contractual autonomy toward a rights-based regulatory model that prioritizes digital inclusion and non-discrimination in access to online services. The legal impact of the bill would be to prohibit a widespread market practice that disproportionately affects vulnerable populations, thereby promoting social equality and enhancing the practical accessibility of constitutionally protected rights. In social terms, the bill would likely improve educational access, facilitate economic participation, and strengthen the capacity of individuals to interact with public institutions and services online. By restricting telecommunications providers' ability to commodify and limit essential digital infrastructure, the proposal affirms the principle that internet access must be guided by public interest rather than market efficiencies alone. Thus, Bill No. 3207/2023 offers a concrete legal mechanism for addressing Brazil's persistent digital divide, elevating connectivity to the status of a protected social right within the country's broader constitutional and statutory framework.

F. Bill No. 4103, of 2024²⁸

- Overview and Legislative Background

Bill No. 4103 of 2024, authored by Senator Ciro Nogueira, proposes significant amendments to Brazil's Marco Civil da Internet (Law No. 12,965/2014), with the aim

28. Projeto de Lei nº 4103, de 2024 (Brazil), Senado Federal, <https://www25.senado.leg.br/web/atividade/materias/-/materia/165939>

of regulating internet applications that facilitate advertisement publication and the intermediation of online purchase and sale transactions. The bill seeks to introduce two new provisions—Articles 7-A and 7-B—creating distinct regimes for platforms that merely enable communication between users for commercial purposes and those that play an active role in transactional processes such as payment or delivery. The justification behind the bill is rooted in widespread concern over consumer fraud in digital marketplaces, particularly scams perpetrated through targeted advertising on social media and classified platforms. The proposal responds to this regulatory gap by introducing new transparency and liability rules within Brazil’s foundational internet legislation.

- Status and Legislative Process

As of April 2025, Bill No. 4103/2024 remains under analysis in the Federal Senate and has not yet progressed to plenary debate or voting. It is currently awaiting the appointment of a rapporteur within the Communication and Digital Law Commission (CCDD), after which it will proceed to the Transparency and Consumer Protection Committee (CTFC) for a final decision. No amendments were submitted during the statutory period, and the legislative process remains in its early stages. Nonetheless, the bill has already stimulated public discussion on the adequacy of existing protections against online fraud and the evolving responsibilities of digital platforms in consumer transactions.

- Provisions and Legislative Innovations

The bill’s principal innovation lies in its bifurcated regulatory model. Article 7-A targets platforms that function as digital bulletin boards—hosting classified ads and facilitating communication between users but not participating directly in the transaction. These platforms are required to inform users that the transaction is conducted between individuals, to disclose profile data such as the user’s registration date, transaction history, and reviews, and to maintain a complaint mechanism when operating professionally. However, such platforms remain exempt from liability for any contract breaches or damages arising from user-to-user transactions, thereby preserving the intermediary protections codified in Article 19 of the Marco Civil.

By contrast, Article 7-B introduces stricter obligations for platforms that act as intermediaries in digital transactions, particularly those that process payments or manage logistics. These platforms must provide consumers with a statutory seven-day withdrawal period, akin to the right of repentance in traditional consumer law. They must also disclose user history data prior to the conclusion of a transaction, offer accessible communication and complaints mechanisms, and cooperate with public enforcement bodies. Most significantly, Article 7-B imposes joint liability on platforms for the delivery of goods and services, a marked departure from the general principle of intermediary non-liability in the digital context. These innovations reflect a deliberate incorporation of consumer protection principles, as seen in Brazil's Consumer Protection Code (CDC), into the architecture of internet governance.

- Relation to the Marco Civil da Internet

Bill No. 4103/2024 represents a functional expansion of the Marco Civil da Internet's normative scope. Originally conceived as a charter for the protection of civil liberties in digital environments—with a particular emphasis on privacy, freedom of expression, and net neutrality—the Marco Civil was not designed to govern the dynamics of e-commerce or online consumer protection. The proposed amendments, however, blur the boundary between internet governance and consumer regulation by introducing transactional transparency obligations and liability rules typically found in specialized legislation. In doing so, the bill hybridizes the Marco Civil's structure, transforming it from a rights-based internet charter into a more operational framework for digital commerce governance. While the bill preserves the intermediary liability shield for passive platforms, it introduces a new legal standard for platforms that engage in active transactional intermediation, thereby creating a dual-track liability regime within the same statute.

- Potential Legal and Social Impact

The enactment of Bill No. 4103/2024 would constitute a significant doctrinal and regulatory shift in Brazil's approach to digital commerce and platform governance. Legally, the bill would impose differentiated obligations based on a platform's degree of involvement in transactions, requiring providers to assess their functional role

with precision. This would necessitate new compliance mechanisms, such as profile verification systems, user history disclosure protocols, and cooperation agreements with public enforcement agencies. The expansion of joint liability to digital intermediaries also introduces new litigation risks, particularly for start-ups and smaller platforms, potentially raising constitutional questions around freedom of enterprise and the proportionality of imposed burdens.

From a social standpoint, the bill aims to enhance consumer confidence in digital markets by increasing transparency and accountability. It addresses the informational asymmetries that frequently underlie digital fraud, particularly in low-trust online environments, and seeks to build a legal framework capable of deterring predatory commercial practices. While the proposal enhances consumer protection, it also provokes important normative debates about the future trajectory of Brazil's digital regulation—namely, whether the Marco Civil should remain a liberal rights-based framework or evolve into a regulatory instrument for market governance. If passed, the bill would exemplify a convergence of internet law and consumer protection law, reinforcing the idea that digital platforms are not only technical intermediaries but also normative actors within the commercial public sphere.

G. Bill No. 295 of 2025²⁹

- Overview and Legislative Background

Senate Bill No. 295 of 2025, authored by Senator Carlos Viana (PODEMOS/MG), introduces a critical intervention in Brazil's evolving legal framework for digital governance and public ethics. Filed on 5 February 2025, the bill seeks to amend two foundational statutes—Law No. 12.965/2014 (Marco Civil da Internet) and Law No. 8.429/1992 (Administrative Misconduct Law)—to prohibit the monetization of digital platforms by political agents during their term of office. The proposal responds to mounting concerns regarding the intersection of public authority and private economic interest in the digital age, particularly where elected officials exploit the

29. Projeto de Lei nº 295, de 2025 (Brazil), Senado Federal, https://www25.senado.leg.br/web/atividade/materias/-/materia/167126#tramitacao_11004934

visibility and institutional legitimacy of their office to generate income from social media platforms and other digital channels.

- Status and Legislative Process

As of 2 May 2025, the bill remains in the preliminary stages of the legislative process, with its most recent status marked as “Waiting for Dispatch” in the Plenary of the Federal Senate. The full text was published in the Senate Journal following its presentation in the legislative session of 5 February. No rapporteur has been appointed, and the bill has not yet been assigned to a committee for analysis, leaving its future trajectory contingent upon legislative prioritization and political alignment.

- Provisions and Legislative Innovations

Bill No. 295/2025 introduces two core amendments. First, it proposes an addition to the Marco Civil da Internet explicitly prohibiting political agents—defined as individuals holding elected or appointed public office—from engaging in the monetization of digital platforms, including blogs, websites, social media profiles, and other internet applications. Monetization is broadly understood to include advertising, sponsorship, affiliate marketing, and other mechanisms of revenue generation. This measure directly targets the commercialization of online engagement by political figures while in office.

Second, the bill amends Law No. 8.429/1992 (the Administrative Misconduct Law) to classify monetization of digital platforms by political agents as an act of administrative misconduct. If enacted, this amendment would subject violators to a range of penalties already enumerated in the statute, including fines, suspension of political rights, and removal from office. By legally equating platform monetization with public impropriety, the bill aims to resolve ambiguities regarding the permissibility and consequences of such conduct, transforming what is currently a political or ethical issue into a justiciable infraction.

- Relation to the Marco Civil da Internet

The bill represents a novel recalibration of the principles enshrined in the Marco

Civil da Internet. While the existing framework champions user rights such as freedom of expression, net neutrality, and data protection (see Articles 3, 7, and 9), it does not presently distinguish among users based on public office, nor does it restrict monetization or economic activity conducted via internet platforms. Article 7 of the Marco Civil protects users' rights to apply consumer protection laws in digital contexts, but without reference to their status or institutional function.

Bill No. 295/2025 introduces a limited and status-based carve-out from this general protection. Rather than restricting user freedoms in a broad sense, the proposal targets a specific category of users—political agents—whose institutional authority, visibility, and access to public platforms pose unique risks to the ethical governance of digital space. It seeks to harmonize the Marco Civil's user-centric ethos with constitutional principles applicable to public administration, including legality, impersonality, morality, and efficiency. In doing so, it shifts the focus from the neutrality of the network to the normative obligations of public office.

- Potential Legal and Social Impact

The legal and social implications of the bill are considerable. By prohibiting public officials from monetizing their digital presence during their term of office, the bill seeks to prevent conflicts of interest, preserve the non-commercial character of public authority, and deter the commodification of institutional influence. In a digital environment increasingly shaped by influencer culture and algorithmically amplified visibility, the risk of political messaging being subsumed under commercial logic is real and growing. The bill positions itself as a normative safeguard against this trend, defending the principle that public service should not be leveraged for personal enrichment via digital means.

Moreover, the linkage of monetization practices to administrative misconduct raises the stakes of non-compliance significantly. Political agents who engage in commercial activities on digital platforms could face the full range of sanctions under the Administrative Misconduct Law, including the loss of office and political rights. This aligns Brazil's legal posture with global trends emphasizing the ethical boundaries of public communication in online spaces. Although the measure restricts expressive and economic freedoms for a defined class of users, it does so in pursuit of

a broader constitutional objective: the integrity and impartiality of public administration.

From a systemic perspective, the bill represents a convergence between digital law and administrative law, illustrating the adaptive capacity of Brazil's legislative framework in responding to new forms of political behavior facilitated by technology. It also foregrounds a critical debate: whether digital visibility acquired through public office can or should be treated as a monetizable asset. If enacted, Bill No. 295/2025 may set a precedent not only for Brazil but for other jurisdictions grappling with the ethical and regulatory dilemmas posed by the digitalisation of politics.

H. Bill No. 880, of 2025³⁰

- Overview and Legislative Background

Senate Bill No. 880 of 2025, introduced by Senator Marcos do Val (PODEMOS/ES), proposes a substantive amendment to Brazil's internet governance statute, the Marco Civil da Internet (Law No. 12.965/2014). The bill was prompted by alarming increases in the dissemination of child sexual abuse material (CSAM) across digital platforms, particularly within encrypted or minimally moderated environments such as Telegram.

Drawing upon international best practices, including those articulated in the IC-MEC's *Model Legislation & Global Review*, the proposal aims to enhance Brazil's regulatory framework by embedding mandatory, proactive content moderation mechanisms into internet law. The bill was filed in early 2025 and is currently pending consideration in the Federal Senate. While it has yet to advance to committee analysis or plenary debate, its submission reflects mounting political and social pressure to strengthen online protections for minors.

- Provisions and Legislative Innovations

The bill seeks to insert Article 21-A into Section III, Chapter III of the Marco Civil

30. Bill No. 880, 2025 (Brazil), <https://www25.senado.leg.br/web/atividade/materias/-/materia/167490>

da Internet, creating a set of positive legal duties for internet application providers. These duties include the implementation of technological tools capable of detecting sexually explicit or pornographic content involving children or adolescents—including digitally altered or simulated materials. Platforms must not only remove such content immediately upon detection but must also notify the user responsible, provide a reasoned justification, and afford an opportunity to contest the decision, thereby respecting procedural fairness while prioritizing child protection.

Beyond content removal, the bill mandates that platforms report detected CSAM to the appropriate authorities, such as the police or the Public Prosecutor's Office. This report must include relevant user data and content evidence, enabling criminal investigations to proceed without delay. Failure to comply with these obligations will trigger the sanctions already set forth in Article 12 of the Marco Civil, while also exposing platforms to civil, criminal, or administrative liability under broader statutory frameworks.

This legislative initiative reflects a distinct shift in Brazil's approach to intermediary liability. Rather than relying solely on reactive models—such as judicial notice-and-takedown procedures—it imposes *ex ante* obligations grounded in technological capability and systemic monitoring. The focus on detecting both actual and simulated content addresses contemporary challenges posed by AI-generated imagery, which often evades traditional moderation techniques.

- Relation to the Marco Civil da Internet

The bill builds upon and extends the rights and responsibilities framework established by the Marco Civil da Internet. Whereas the original statute prioritized principles such as net neutrality, user privacy, and limited intermediary liability (particularly under Articles 3, 7, and 19), Bill No. 880/2025 reorients the balance toward a duty of care that obliges platforms to act preemptively in the presence of egregious harms such as CSAM. Article 21-A would operate alongside, rather than in contradiction to, existing provisions, reinforcing the statute's protective ethos through more concrete enforcement mechanisms.

In doing so, the bill reconfigures the scope of platform neutrality in cases involving severe human rights violations. The proposed duty to monitor, detect, and report

unlawful content carves out an exception from the general principle of provider immunity for user-generated content. While Article 19 of the Marco Civil conditions platform liability on the existence of a court order, Article 21-A introduces autonomous duties rooted in the intrinsic illegality of the material in question and the pressing need to safeguard vulnerable individuals.

The bill also pre-empts potential conflicts with the General Data Protection Law (Lei Geral de Proteção de Dados – LGPD, Law No. 13.709/2018). By invoking the exemption clause in Article 4, III(d) of the LGPD, which permits data processing for the purposes of public security and criminal investigations, the bill clarifies that the transfer of personal data to law enforcement in cases involving CSAM does not violate Brazil’s data protection framework.

- Potential Legal and Social Impact

If enacted, Bill No. 880/2025 would mark a decisive evolution in Brazil’s regulatory response to online child sexual exploitation. It responds to a quantifiable surge in digital CSAM activity: according to data from SaferNet, a Brazilian NGO focused on digital rights, there was a 78% increase in reports of CSAM dissemination on Telegram between the first and second semesters of 2024. The number of active groups rose from 874 to 1,043, with over 2 million users implicated in the dissemination or sale of such material. These statistics expose the inadequacy of voluntary moderation and underscore the need for legal mandates that operationalize platform responsibility.

The bill’s impact would be both normative and operational. It reinforces the notion that internet governance must serve as an instrument for the protection of human dignity, especially where minors are concerned. It also shifts the legal narrative from reactive liability to proactive prevention, making Brazil one of the few democracies to explicitly mandate content detection and reporting technologies for CSAM.

By aligning national law with international soft law benchmarks, the bill strengthens Brazil’s standing in global efforts to eliminate online child exploitation. It also raises significant implementation challenges, including the need for platforms to invest in advanced monitoring technologies and train moderation teams capable of handling complex, often encrypted content environments. Smaller providers may

struggle to meet these obligations without regulatory guidance or technical support, suggesting the potential need for secondary regulations or public-private partnerships.

Ultimately, Bill No. 880/2025 reinforces the *Marco Civil da Internet*'s foundational commitment to a rights-based digital order while addressing emergent threats that require more than passive compliance. It represents a recalibration of internet law in favor of vulnerable users and sets a precedent for further integration between child protection, platform accountability, and criminal enforcement in the Brazilian legal system.

VI. CONCLUSION

In conclusion, Brazil's *Marco Civil da Internet* (Law No. 12.965/2014) has undergone significant legislative evolution since its enactment in 2014, particularly through amendments like the introduction of the *Lei Geral de Proteção de Dados Pessoais* (LGPD) in 2018. The LGPD enhanced user privacy protections and data processing regulations, complementing the *Marco Civil*'s foundational principles of net neutrality, user rights, and data retention. These changes solidified the law's role in protecting user privacy and governing internet platforms, ensuring Brazil's alignment with international data protection standards. Additionally, the *Decree No. 8,771/2016* and subsequent amendments clarified enforcement mechanisms, making the law more actionable and comprehensive.

The potential future changes through the proposed bills will significantly impact the scope and enforcement of Brazil's internet regulations. For example, Bill No. 2922/2020 introduces an innovative approach by holding digital platforms financially accountable for content they monetize, such as disinformation and hate speech. This bill would mark a substantial shift from the traditional content liability model of the *Marco Civil*, introducing an economic deterrent for platforms that profit from harmful content. The passage of this bill could dramatically reshape Brazil's digital ecosystem by addressing the financial incentives that drive the spread of false and harmful information.

Similarly, Bill No. 2821/2022 seeks to address algorithmic discrimination by mandating platforms to implement mechanisms to identify and mitigate algorithmic bias.

This bill would impose a new layer of responsibility on digital platforms, requiring them to proactively address issues of fairness in automated decision-making processes. If passed, it could set a precedent for digital governance, where platform operators are held accountable not only for the content they host but also for the algorithms they deploy, ensuring that these algorithms do not perpetuate discrimination.

Moreover, Bill No. 4103/2024 would impose new transparency and liability rules on digital platforms involved in commercial transactions, addressing consumer fraud in digital marketplaces. It would introduce a differentiated liability regime, particularly for platforms facilitating transactions. This amendment would strengthen consumer protection by requiring platforms to disclose more information about sellers and ensure more transparent processes in digital commerce. If enacted, this bill could lead to enhanced trust in Brazil's digital economy and reduce the risk of fraud, particularly for vulnerable users in online environments.

The potential changes highlighted by these bills is important because it provides a comprehensive understanding of how Brazil's legal framework is adapting to new technological and societal challenges. It not only informs Brazilian legal and policy debates but also serves as a valuable resource for international policymakers and legal scholars looking to navigate the complex landscape of digital governance. By exploring the intersection of law, technology, and society, this research contributes to shaping a more just and equitable digital future globally.

REFERENCES

A Legislation, Decrees and Parliamentary Debates

Lei nº 12.965 de 23 de abril de 2014 (Brazil), 'Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil' (24 April 2014) *Diário Oficial da União* 1, <https://legislacao.presidencia.gov.br/atos/?tipo=LEI&numero=12965&ano=2014&ato=93eUTRE9ENVpWTdb6>.

Lei No 13.709, de 14 de agosto de 2018, https://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm#art65.

Lei No 13.853, de 8 July 2019, https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm#art1.

Decreto nº 8.771, de 11 de maio de 2016 (Brazil), 'Regulamenta a Lei nº 12.965, de 23 de abril de 2014' (11 May 2016) *Diário Oficial da União* 7.

Medida Provisória nº 1.068, de 6 de setembro de 2021, https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2021/Mpv/mpv1068.htm#art1.

Senado Federal, *Ata da Sessão Deliberativa do PLC 21/2014*, 22 April 2014.

Senado Federal (Brazil), 'Entenda o Projeto de Marco Civil da Internet' (Web Page, 3 September 2013) <https://www12.senado.leg.br/noticias/materias/2013/09/03/entenda-o-projeto-de-marco-civil-da-internet> accessed 3 March 2025.

B Bills

Projeto de Lei nº 3207, de 2023 (Brazil), *Senado Federal*, https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm accessed 15 February 2025.

Bill No. 2922, 2020 (Brazil), <https://www25.senado.leg.br/web/atividade/materias/-/materia/142129>.

Bill No. 2184, 2022 (Brazil), <https://www25.senado.leg.br/web/atividade/materias/-/materia/154315>.

Bill No. 3207, 2023 (Brazil), Senado Federal, <https://www25.senado.leg.br/web/atividade/materias/-/materia/158369>.

Bill No. 4103, 2024 (Brazil), Senado Federal, <https://www25.senado.leg.br/web/atividade/materias/-/materia/165939>.

Bill No. 880, 2025 (Brazil), <https://www25.senado.leg.br/web/atividade/materias/-/materia/167490>.

Bill No. 295, 2025 (Brazil), Senado Federal, https://www25.senado.leg.br/web/atividade/materias/-/materia/167126#tramitacao_11004934.

Senado Federal, *Projeto de Lei nº 3207*, <https://www25.senado.leg.br/web/atividade/materias/-/materia/165939>.

Projeto de Lei nº 2821/2022 (Brazil), *Senado Federal*, 21 November 2022, https://www25.senado.leg.br/web/atividade/materias/-/materia/155169#tramitacao_10358709.

C Literature

Carlos Affonso Pereira de Souza, Fabro Steibel and Ronaldo Lemos, 'Notes on the Creation and Impacts of Brazil's Internet Bill of Rights' (2017) 5(1) *The Theory and Practice of Legislation* 73.

Guilherme Francisco Waterloo Radomsky and Fabrício Solagna, 'Marco Civil da Internet: Abrindo a Caixa-Preta da Agenda de uma Política Pública' (2016) 12(1) *Liinc em Revista* 154.

Laura Vilela Rodrigues Rezende and Meyrielle Rodrigues de Lima, 'Governança Na Internet: Um Estudo Sobre o Marco Civil Brasileiro' (2016) 19(1) 133 <https://dialnet.unirioja.es/descarga/articulo/6499302.pdf>.

Maria Alejandra Nicolás et al, 'A Primeira Fase da Consulta Pública da Regulamentação do Marco Civil da Internet: Estrutura Comunicativa, Limites e Contribuições' (2017) 15(2) *Contemporânea | Comunicação e Cultura* 485, 486; Soraia Herrador Costa Lima de Souza, *Internet Policy Framing*

in Emerging Economies: A Case Study of Marco Civil da Internet, A Brazilian Law for Internet Governance (Social Science Research Network, 1 December 2016).

Rachel Callai Bragatto, Rafael Cardoso Sampaio and Maria Alejandra Nicolás, 'Inovadora e democrática. Mas e aí? Uma análise da primeira fase da consulta online sobre o Marco Civil da Internet' (2015) 14(29) *Política & Sociedade* 125.

Raphael Silveiras and Gilda Figueiredo Portugal Gouvea, 'A presença do Estado na rede: Marco Civil da Internet e reforma da Lei de Direito Autoral' (2016) 12(1) *Liinc em Revista* 132.

Samuel Anderson Rocha Barros, 'Os desafios das consultas públicas online: lições do Marco Civil da Internet' (2016) 12(1) *Liinc em Revista* 72.

II
PERÍCIA FORENSE
COMPUTACIONAL

MARCO CIVIL DA INTERNET E PROVA DIGITAL: AVANÇOS E LIMITAÇÕES

Leonardo Andrade Macedo

Mestre e Doutorando em Direito pela UFMG

Procurador da República

DOI: <https://doi.org/10.59224/dti7.ch2>

Resumo: Este artigo analisa os avanços do Marco Civil da Internet na regulamentação da prova digital associada às comunicações pela internet, destaca discussões relevantes do tema na jurisprudência dos tribunais superiores no Brasil e aponta as omissões e deficiências da legislação atual. Ao final, conclui-se pela necessidade de aperfeiçoamento legislativo, especialmente quanto aos parâmetros para acesso a dados de conteúdo armazenados, a fim de garantir maior segurança jurídica e proteção dos direitos fundamentais no ambiente digital.

Palavras-chave: Marco Civil da Internet; prova digital; sigilo de dados.

Abstract: *This article examines the progress of Brazilian Civil Rights Framework for the Internet in regulating digital evidence in online communications, highlighting key discussions in the case law of superior courts and identifying gaps and shortcomings in current legislation. It concludes by stressing the need for legislative improvements, particularly in defining clear parameters for accessing stored content data, to enhance legal certainty and strengthen the protection of fundamental rights in the digital environment.*

Keywords: *Brazilian Civil Rights Framework for the Internet; digital evidence; data secrecy.*

SUMÁRIO: 1. Introdução. 2. Tipos de dados e obtenção de provas digitais nas comunicações pela internet 2.1 Dados cadastrais. 2.2 Dados de tráfego. 2.3 Dados de conteúdo. 3. Conservação dos dados nas comunicações pela internet. 3.1 Guarda de dados (*data retention*). 3.2 Preservação de dados (*data preservation*). 4. Conclusão. Referências.

1. INTRODUÇÃO

Os avanços tecnológicos das últimas décadas e a popularização da tecnologia

produziram um novo paradigma de interação entre humanos e computadores, conhecido como “computação ubíqua” ou “computação pervasiva”, caracterizado pela integração de tecnologias no cotidiano das pessoas, de forma natural e onipresente.¹ Dispositivos computacionais ditos “inteligentes”, como notebooks, tablets, telefones, relógios, câmeras e televisores (para ficar apenas nos tipos mais comuns de IoTs),² estão presentes em todo lugar, conectados permanentemente à internet, coletando e armazenando uma quantidade massiva de dados, de forma automática, ininterrupta e quase imperceptível.³

Essa nova realidade impõe graves riscos para os direitos fundamentais, não apenas pela possibilidade de intervenções abusivas do Estado - como certas técnicas de

-
1. A expressão “*computação ubíqua*” foi usada pela primeira vez pelo cientista da computação norteamericano Mark Weiser em 1988 e publicada em 1991 no artigo *The Computer for the 21st Century*. WEISER, Mark. The Computer for the 21st Century. *Scientific American*, 265, September 1991, p. 94-104. Também se utiliza a expressão “*inteligência ambiental*” ou apenas AmI (*Ambient Intelligence*) para se referir a uma visão na qual os humanos estão cercados pela computação e tecnologias de redes em todos os ambientes.
 2. Sílvia Meira define coisas conectadas (IoT) como “objetos digitais completos”, por serem dispositivos com possibilidade de computação, comunicação e controle (MEIRA, Sílvia. *Sinais do futuro imediato, #1: internet das coisas*. Ikewai, Recife, dez. 2016). Ele aponta 10 características das IoT: “[1] são identificáveis e endereçáveis, estão em rede; [2] são programáveis, mesmo as mais rudimentares; [3] têm memória, [4] sensores, pra capturar sinais ao seu redor, podem ter [5] atuadores, para agir sobre seu ambiente, [6] são rastreáveis, podemos saber onde estão e por onde estiveram... [7] podem estabelecer conexões com outras coisas, pessoas e organizações, assim como [8] relacionamentos, para formar redes, grupos, comunidades, onde poderão realizar [9] interações com outros agentes aos quais podem se [10] associar, para realizar tarefas mais complexas do que uma única coisa poderia.” MEIRA, Sílvia. *23 anotações sobre 2023 [x] – 5G & a internet das coisas*. Disponível em: <https://silvio.meira.com/silvio/23-anotacoes-sobre-2023-x/>. Acesso em: 03 fev. 2025.
 3. MAGRANI, Eduardo. Threats of the Internet of Things in a techno regulated society: A New Legal Challenge of the Information Revolution. In: *Orbit Journal*. Vol 1. Issue 1. 2017, p. 1-17.

vigilância algorítmica,⁴ *hackeamento* estatal e infiltração por *malware* -,⁵ mas principalmente por parte de grandes agentes econômicos do setor de tecnologia (*big techs*), que se aproveitam da profunda assimetria informacional e de poder em relação aos usuários e se valem de expedientes pouco transparentes para utilizar essa gigantesca massa de dados em prol de seus interesses privados, inaugurando uma verdadeira “*era do capitalismo de vigilância*”, como alerta Shoshana Zuboff.⁶

Por outro lado, nos campos da investigação forense e do direito probatório, todos esses rastros deixados na interação tecnológica compõem uma rica fonte de informações, capazes de auxiliar na reconstrução de fatos. Esses dados, associados a outros elementos de prova tradicionais, podem revelar onde alguém esteve, em que momento, por quanto tempo, seus deslocamentos, quem estava junto, com quem se

4. “A vigilância algorítmica é entendida como um ‘novo tipo de vigilância’ que emprega ‘novas ferramentas’ e consequentemente ‘automatiza’ o processamento de dados. (...) Hoje em dia, é possível usar algoritmos para fazer ‘predictive policing’, ‘risk profiling’ and ‘preemptive surveillance’. Isto demonstra que há uma mudança nos programas de vigilância, graças às novas tecnologias, que passaram a ser preventivos e preditivos.” MELO, Isabella Gabriele Campelo de, *Direito à privacidade na era digital: a vigilância estatal algorítmica da comunicação no sistema europeu de direitos humanos*, Dissertação: Coimbra, 2024, p. 2-4.
5. No *hacking* estatal há a infiltração em dispositivos e sistemas por meio de falhas e aberturas previamente identificadas, mediante conexão com a internet (“acesso remoto não autorizado”). Já na infiltração por *malware* ocorre a instalação de programas no sistema ou dispositivo alvo para abertura de um acesso remoto, denominado “mecanismo de acesso excepcional” (*backdoor*). Essas técnicas implicam um enorme grau de afetação de direitos fundamentais, viabilizando ações de acompanhamento da geolocalização em tempo real, captação ambiental (por meio do acesso à câmera e microfone do dispositivo), interceptação do fluxo de mensagens de correio eletrônico e aplicativos, busca por dados armazenados e vigilância on-line. Atualmente, há, inclusive, certos *softwares* espiões (*spywares*), como o Pegasus e o Graphite, que viabilizam o acesso remoto aos aparelhos sem a necessidade de qualquer ação por parte do titular, uma estratégia denominada “zero clique”. SMANIO, Gianluca Martins. *Vigilância policial em meio digital: entre o garantismo e a eficiência*. Curitiba: Juruá, 2022, p. 192-193. RAMALHO, David Silva. *Métodos ocultos de investigação criminal em ambiente digital*, Coimbra: Almedina, 2017, p. 320 a 322. TILT UOL, *Como agia app espião de Israel que hackeou o WhatsApp de civis sem clicar...* 06/02/2025, Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2025/02/06/como-agia-app-espiao-de-israel-que-hackeou-o-whatsapp-de-civis-sem-clicar.html>. Acesso em 07 fev. 2025.
6. ZUBOFF, Shoshana. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs, 2019.

comunicou e interagiu, com que frequência, que tipos de pesquisas fez na internet, quais sites visitou, sem falar do conteúdo de e-mails, documentos, agenda de contatos e grupos, mensagens de texto, áudio e vídeos, formando o que se denomina prova digital.

A prova digital (*"digital evidence"*) pode ser conceituada como *"os dados em forma digital (no sistema binário) constantes de um suporte eletrônico ou transmitidos em rede de comunicação, os quais contêm a representação de fatos ou ideias"*.⁷ Essa expressão é usada tanto para designar "fonte de prova", entendida como *"pessoas ou coisas das quais pode-se conseguir a prova (rectius, o elemento de prova)"*, como também no sentido de "elemento de prova", isto é, *"dados objetivos que confirmam ou negam uma asserção a respeito de um fato que interessa à decisão da causa"*.⁸

Esse tipo de prova se caracteriza pela imaterialidade e volatilidade, pois os dados em formato digital são meros impulsos de corrente elétrica, frágeis e passíveis de modificação por simples alteração da sequência numérica, sendo necessário o uso de equipamentos para transformação dos dados em linguagem natural compreensível ao homem. Além disso, as informações não estão limitadas ao suporte físico original, podendo ser transferidas e copiadas para outros dispositivos, de forma fiel, idêntica e infinita, sem perder sua essência.⁹

Essas características da prova digital exigem que sejam tomados vários cuidados procedimentais para garantir sua confiabilidade, integridade e autenticidade.¹⁰ Nesse sentido, a Lei nº 13.964/2019 introduziu disposições no Código de Processo Penal (artigo 158-A e seguintes) acerca da cadeia de custódia, que devem ser observadas

7. VAZ, Denise Provasi. *Provas digitais no processo penal: formulação do conceito, definição das características e sistematização do procedimento probatório*. Tese (Doutorado em 2012) – Faculdade de Direito da Universidade de São Paulo, São Paulo, 2012, p. 63.

8. GOMES FILHO, Antonio Magalhães. Notas sobre a terminologia da prova (reflexos no processo penal brasileiro). In: YARSHELL, Flávio Luiz; DE MORAES, Zanoide (Coords.). *Estudos em Homagem à Professora Ada Pellegrini Grinover*. São Paulo: Editora DPJ, 2005, p. 308.

9. SAAD, Marta; ROSSI, Helena Costa; PARTATA, Pedro Henrique, A obtenção das provas digitais no processo penal demanda uma disciplina jurídica própria? Uma análise do conceito, das características e das peculiaridades das provas digitais, *Revista Brasileira de Direito Processual Penal*, v. 10, n. 3, 2024, p. 5-6.

10. BADARÓ, Gustavo. Os standards metodológicos de produção na prova digital e a importância da cadeia de custódia. *Boletim IBCCRIM*, São Paulo, ano 29, n. 343, jun. 2021, p. 7.

em todas as etapas de produção da prova, desde o reconhecimento, coleta, acondicionamento, transporte, processamento, armazenamento e descarte dos vestígios, sob pena dela ter sua validade questionada e não ser admitida em juízo. Também merece destaque a norma técnica ABNT ISO/IEC 27037:2013, que apresenta diretrizes para identificação, coleta, aquisição e preservação da evidência digital.

Porém, para intervenções que implicam restrições relevantes a direitos fundamentais, não basta simplesmente observar as regras da cadeia de custódia. A legitimidade da intervenção em direitos fundamentais, de modo geral, deve ser aferida a partir do princípio constitucional da proporcionalidade,¹¹ com a análise da aptidão da medida para alcançar o fim proposto (adequação), o exame da necessidade da providência ante a ausência de alternativas menos gravosas para se atingir o resultado (necessidade) e a ponderação entre, de um lado, os benefícios que se pretende alcançar com a medida e, de outro, a gravidade da limitação imposta ao direito fundamental (proporcionalidade em sentido estrito).¹²

Atualmente, diante da massiva quantidade de informações coletadas, armazenadas e processadas e do fluxo intenso de dados pessoais, a concepção individualista do direito à privacidade, associada a uma liberdade negativa oponível ao Estado, não se mostra mais adequada e suficiente.¹³ Nesse cenário, o direito à privacidade passa a

11. BARROSO, Luís Roberto. *Curso de Direito Constitucional contemporâneo*. 8ª ed., São Paulo: Saraiva, 2019, p. 512.

12. GLEIZER; Orlandino. *Busca estatal por informações digitais e intervenções em direitos fundamentais no processo penal*: A 1ª parte da análise sobre quatro casos mencionados em reportagem do JOTA. 2019. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/penal-em-foco/busca-estatal-por-informacoes-digitais-e-intervencoes-em-direitos-fundamentais-no-processo-penal>. Acesso em: 04 fev. 2025.

13. A origem histórica do direito à privacidade é identificada no artigo de Samuel Warren e Louis Brandeis, intitulado "The right to privacy", publicado em 1890 na *Harvard Law Review*, acerca dos limites para exposição da imagem das pessoas na imprensa, em que se conclui que essa proteção deriva da inviolabilidade da personalidade, consistindo em um "direito de ser deixado só" (WARREN, Samuel; BRANDEIS, Louis. The right to privacy. *Harvard Law Review*, v. 4, n. 5, pp. 193-220, 1890). Essa concepção individualista de privacidade dialoga com os conceitos tradicionais da doutrina brasileira, como o adotado por Tércio Sampaio Ferraz Júnior, que entende privacidade como a faculdade de impedir que terceiros tenham acesso a esferas exclusivas do particular (FERRAZ JÚNIOR, Tércio Sampaio. *Sigilo de dados*: o direito à privacidade e os limites à função fiscalizadora do Estado. *Revista da Faculdade de Direito da Universidade de São Paulo*. São Paulo, v.

exigir do Estado - e também dos demais particulares, sujeitos à eficácia horizontal dos direitos fundamentais - prestações positivas para conferir ao indivíduo um efetivo controle sobre as próprias informações, como pressuposto para o livre desenvolvimento de sua personalidade. O direito à privacidade assume uma dimensão coletiva e relacional, dialogando com os direitos à autodeterminação informativa e à proteção dos dados pessoais, voltados a garantir uma ordem comunicacional livre e democrática, conforme já reconhecido pelo Tribunal Constitucional Alemão no paradigmático julgamento sobre a Lei do Censo de 1983.¹⁴

A preservação da privacidade nesse novo contexto foi um dos três eixos que pausaram as discussões durante o processo legislativo do Marco Civil da Internet (MCI, Lei 12965/2014).¹⁵ E, de fato, o texto final do MCI acabou por introduzir, de forma inovadora no ordenamento jurídico brasileiro, normas voltadas à preservação da privacidade e à proteção de dados pessoais no ambiente da internet.¹⁶

88, jan./dez. 1993, p. 439-459).

14. SARLET, Ingo Wolfgang. *Proteção de dados pessoais como direito fundamental na Constituição Federal brasileira de 1988*: contributo para a construção de uma dogmática constitucionalmente adequada. Direitos Fundamentais e Justiça. Belo Horizonte, v.14, n.42, jan./jun. 2020, p. 190.
15. O tripé do MCI era formado, além da preservação da privacidade, pela garantia da liberdade de expressão (responsabilização das plataformas por conteúdo de terceiros) e a neutralidade da rede. COSTA, Gilberto Ferreira. *Regulação e governança de internet no Brasil: a jurisprudência do Superior Tribunal de Justiça sobre o Marco Civil da Internet*. Dissertação de mestrado. Brasília: UNB, 2024.
16. “O texto aprovado pelo Congresso apresenta diferenças significativas em relação à proposta inicial do Executivo. Uma das diferenças mais evidentes é a quantidade e especificidade de normas relacionadas à privacidade e à proteção de dados presentes no texto final, que não constavam da proposta inicial. Enquanto a primeira versão trazia o direito à privacidade como princípio e regra geral da disciplina do uso da internet no país, a Lei 12.965/2014 acabou por disciplinar de forma bastante específica a proteção de dados na internet, estabelecendo normas sobre danos morais e materiais em caso de violação da intimidade e vida privada (art. 7.º, I), a inviolabilidade e sigilo do fluxo de comunicações e das comunicações privadas armazenadas (art. 7.º, II e III), o direito ao não fornecimento a terceiros de dados pessoais salvo mediante consentimento do usuário (art. 7.º, VII), a exclusão definitiva dos dados pessoais fornecidos a determinada aplicação de internet (art. 7.º, X), a publicidade e clareza de eventuais políticas de uso dos provedores de conexão e de aplicações (art. 7.º, XI), entre outras.” (MENDES, Laura Schertel. O diálogo entre o Marco Civil da Internet e o Código de Defesa do Consumidor. *Revista de Direito do Consumidor*. vol. 106, ano

Assim, passada mais de uma década desde o advento do Marco Civil da Internet, este trabalho se propõe a analisar os avanços trazidos por essa lei para a preservação da privacidade no campo das provas digitais, bem como as limitações e desafios ainda existentes nesse seara, a partir da jurisprudência dos tribunais superiores. Nessa análise, também serão mencionados outros diplomas normativos, como a Lei de Interceptações Telefônicas e Telemáticas (Lei 9296/1996), a Lei Geral de Proteção de Dados (LGPD, Lei 13709/2018) e a Convenção de Budapeste sobre Cibercriminalidade (Convenção de Budapeste),¹⁷ que dialogam com o MCI e formam um verdadeiro micro-sistema da prova digital.

2. TIPOS DE DADOS E OBTENÇÃO DE PROVAS DIGITAIS NAS COMUNICAÇÕES PELA INTERNET

No Brasil, a definição legal de "*internet*" consta da Portaria n. 148, de 31/05/1995, do Ministério das Comunicações, que aprovou a Norma 4/1995, regulamentando o uso da rede pública de telecomunicações para acesso à internet. O item 3 da norma estabelece que a internet é um "nome genérico que designa o conjunto de redes, os meios de transmissão e comutação, roteadores, equipamentos e protocolos necessários à comunicação entre computadores, bem como o 'software' e os dados contidos nestes computadores."¹⁸

Por sua vez, a Lei 9296/1996 distingue sistemas de informática e telemática (art. 1º, § único). Os sistemas de informática (ou computador) são aqueles que fazem a coleta, armazenamento, transmissão e processamento de informações em meios

25, São Paulo: Ed. RT, jul.-ago. 2016. p. 38).

17. A Convenção de Budapeste sobre Cibercriminalidade foi aprovada no Brasil por meio do Decreto Legislativo 37/2021 e entrou em vigor internacional para o país em 1º de março de 2023, após a conclusão do processo de adesão. O texto foi promulgado por meio do Decreto 11.491/2023 e passou a vigor internamente em 13 de abril de 2023, data da publicação do tratado no Diário Oficial da União.

18. Na mesma linha, Zaniolo define a internet como o "conjunto de redes de computadores mundialmente interligadas, com um grupo de protocolos e serviços em comum - o TCP/IP, de forma que os usuários a ela conectados possam compartilhar serviços de informação e comunicação de alcance global". ZANIOLO, Pedro Augusto. *Crimes modernos: o impacto da tecnologia no Direito*. 4. ed. Salvador: Editora JusPodivm, 2021, p. 172.

digitais.¹⁹ Já os sistemas de telemática combinam tecnologias de informática e telecomunicações.²⁰ A comunicação é telemática quando se realizar de forma digital, ou seja, quando fizer uso da conversão dos dados em séries binárias, se distinguindo nesse aspecto das comunicações telefônica e telegráfica.²¹ Na prática judiciária brasileira, as expressões “quebra de sigilo telemático” ou “quebra de sigilo de dados telemáticos” têm sido utilizadas, sem muito rigor técnico, para designar os diversos meios de obtenção de provas digitais.²²

Nas comunicações (telemáticas) pela internet, ao menos para fins probatórios, os dados podem ser classificados em três categorias: (a) dados cadastrais (*subscriber information*); (b) dados de tráfego (*traffic data*); e (c) dados de conteúdo (*content data*). Essa divisão pode ser extraída tanto do Marco Civil da Internet, como também da Convenção de Budapeste,²³ e reflete uma gradação no nível de afetação do direito à privacidade em intervenções envolvendo esses tipos de dados.²⁴

Passemos, então, à análise de cada categoria de dados e aos parâmetros para obtenção dessas provas digitais.

19. Para os fins da Convenção de Budapeste (art. 1, a), a expressão “sistema de computador” designa “qualquer aparelho ou um conjunto de aparelhos interconectados ou relacionados entre si que asseguram, isoladamente ou em conjunto, pela execução de um programa, o processamento eletrônico de dados.”

20. A telecomunicação está definida no artigo 60, §1º, da Lei 9.472/97, como “a transmissão, emissão ou recepção, por fio, radioeletricidade, meios ópticos ou qualquer outro processo eletromagnético, de símbolos, caracteres, sinais, escritos, imagens, sons ou informações de qualquer natureza”.

21. SIDI, Ricardo. *A interceptação das comunicações telemáticas no processo penal*. Belo Horizonte: Editora D’Plácido, 2016, p. 69-72.

22. QUITO, Carina. As quebras de sigilo telemático no processo penal e o paradoxo do acesso irrestrito às comunicações armazenadas. In: WOLKART, Erik Navarro et al. (coord.). *Direito, processo e tecnologia*. 2. ed. São Paulo: Thomson Reuters Brasil, 2021, p. 165.

23. Na Convenção de Budapeste, os dados de tráfego e de conteúdo são abrangidos pela expressão “dados de computador”, que “designa qualquer aparelho ou um conjunto de aparelhos interconectados ou relacionados entre si que asseguram, isoladamente ou em conjunto, pela execução de um programa, o processamento eletrônico de dados” (art. 1, b).

24. SIDI, Ricardo. *A interceptação das comunicações telemáticas no processo penal*. Belo Horizonte: Editora D’Plácido, 2016, p. 295.

2.1 Dados cadastrais

Os dados cadastrais são informações básicas sobre o usuário dos serviços fornecidos pelos provedores de conexão e de aplicações de internet. Conforme o art. 10, §3º do Marco Civil da Internet, são considerados dados cadastrais a filiação, o endereço e a qualificação pessoal do usuário, entendida esta como nome, prenome, estado civil e profissão, como previsto no art. 11, §2º, do Decreto n. 8.771/2016, que regulamenta o MCI.

Já na Convenção de Budapeste (art. 18.3), a expressão “informações cadastrais do assinante” é um pouco mais abrangente²⁵ e contempla:

“qualquer informação mantida em forma eletrônica ou em qualquer outra, que esteja em poder do provedor de serviço e que seja relativa a assinantes de seus serviços, com exceção dos dados de tráfego e do conteúdo da comunicação, e por meio da qual se possa determinar:

a. o tipo de serviço de comunicação utilizado, as medidas técnicas tomadas para esse fim e a época do serviço;

b. a identidade do assinante, o domicílio ou o endereço postal, o telefone e outros números de contato e informações sobre pagamento e cobrança, que estejam disponíveis de acordo com o contrato de prestação de serviço.

c. quaisquer outras informações sobre o local da instalação do equipamento de comunicação disponível com base no contrato de prestação de serviço.”

25. No âmbito da ADI n. 4906/DF, em que se discute a constitucionalidade do art. 17-B da Lei n. 9.613/1998 (Lei de Lavagem de Capitais), inserido pela Lei n. 12.683/2012, em 11/09/2024, o STF firmou a seguinte tese de julgamento: “É constitucional norma que permite o acesso, por autoridades policiais e pelo Ministério Público, a dados cadastrais de pessoas investigadas independentemente de autorização judicial, excluída do âmbito de incidência da norma a possibilidade de requisição de qualquer outro dado cadastral além daqueles referentes à qualificação pessoal, filiação e endereço (art. 5º, X e LXXIX, da CF)”. Porém, em novembro de 2024, o Procurador-Geral da República opôs embargos de declaração para fins de esclarecimento quanto “à extensão dos dados abrangidos pela ‘qualificação pessoal’ passíveis de requisição direta pelo Ministério Público e por autoridades policiais, em contexto de combate aos crimes cibernético e à luz do item 3 do art. 18 da Convenção de Budapeste”.

Justamente por implicar um menor grau de afetação ao direito à privacidade, a legislação assegura o acesso direto a esses dados pelas autoridades administrativas que detenham competência legal para a sua requisição (art. 10, §3º do MCI e art. 18.1, b da Convenção de Budapeste), dispensando, portanto, a necessidade de ordem judicial.²⁶

Embora o acesso das autoridades administrativas a dados cadastrais não se subordine à reserva de jurisdição, o Decreto n. 8.771/2016 exige que na requisição seja indicado “o fundamento legal de competência expressa para o acesso e a motivação para o pedido de acesso aos dados cadastrais” (art. 11, caput). Além disso, os órgãos da administração pública federal deverão publicar anualmente na internet relatórios estatísticos de requisição de dados cadastrais (Decreto n. 8.771/2016, art. 12).

Já na seara criminal, além da prerrogativa geral conferida ao Ministério Público²⁷ e às autoridades policiais²⁸ de requisitar informações a entidades públicas e particulares, há normas específicas garantindo o acesso direto dessas autoridades a dados cadastrais para fins de persecução de determinados crimes mais graves, como lavagem de dinheiro (art. 17-B da Lei 9.613/1998), crimes praticados por organizações criminosas (art. 15 da Lei 12.850/2013), seqüestro e cárcere privado, redução à condição análoga à de escravo, tráfico de pessoas, extorsão mediante seqüestro e tráfico de criança ou adolescente (art. 13-A do Código de Processo Penal).

Carina Quito entende que, à luz da garantia prevista no art. 5º, X, da Constituição, e reforçada no *caput* do art. 10 do MCI, só nessas hipóteses legais expressamente previstas para crimes de maior gravidade é que seria possível o acesso direto aos dados cadastrais e que a regra geral seria a cláusula de reserva de jurisdição.²⁹ Essa posição teria sido reforçada após a Emenda Constitucional 115/2022, que inseriu explicitamente o direito à proteção de dados pessoais no rol de direitos fundamentais do

26. Por outro lado, no caso de autoridades sem competência legal para requisição ou mesmo particulares, a obtenção dos dados cadastrais dependerá de ordem judicial direcionada aos provedores.

27. Constituição Federal, art. 129, VI; Lei n. 8.625/1993, art. 26, I, “b” e II; Lei Complementar n. 75/1993, art. 8º, II e IV, §2º.

28. Lei 12.830/2013, art. 2º, §2º.

29. QUITO, Carina. As quebras de sigilo telemático no processo penal e o paradoxo do acesso irrestrito às comunicações armazenadas. In: WOLKART, Erik Navarro et al. (coord.). *Direito, processo e tecnologia*. 2. ed. São Paulo: Thomson Reuters Brasil, 2021, p. 175.

art. 5º da Constituição (inciso LXXIX).

Porém, a jurisprudência consolidada do Superior Tribunal de Justiça segue o entendimento de que “os dados cadastrais armazenados nos bancos de dados dos provedores possuem caráter objetivo, assim o acesso direto pelos órgãos de investigação, sem prévia autorização judicial, não viola a garantia constitucional de proteção à intimidade, à vida privada, à honra e à imagem.”³⁰ De fato, embora configurem dados pessoais, nos termos do art. 5º, I, da LGPD, e, como tais, sejam dignos de medidas de proteção, o rol de informações incluídas na categoria dos dados cadastrais é bastante limitado e revela muito pouco da vida privada e da intimidade do indivíduo, estando alguns desses dados, inclusive, disponíveis em bases públicas e fontes abertas na internet.

Diferentemente do que ocorre com certos tipos de dados pessoais mais críticos, em que o sigilo e a reserva de jurisdição estão expressamente previstos na legislação, como dados bancários (art. 1º da Lei Complementar n. 105/2001) e dados fiscais (art. 198 do Código Tributário Nacional), nem a LGPD nem o inciso LXXIX do art. 5º da Constituição estabelecem uma cláusula geral de sigilo para dados pessoais ou subordinam sua obtenção pelas autoridades públicas à reserva de jurisdição. A legislação de proteção de dados apenas impõe que sejam observadas certas condições para o

30. SUPERIOR TRIBUNAL DE JUSTIÇA, *Jurisprudência em teses*: Marco Civil da Internet II - Lei 12.965/2014. Edição n. 223, Brasília, 11 de outubro de 2023. Disponível em <https://scon.stj.jus.br/SCON/jt/jt.jsp>. Acesso em 07 fev. 2025, p. 4. O tema voltou recentemente à pauta do STJ, em caso acerca da obrigação de instituições financeiras fornecerem dados cadastrais de seus correntistas “quando requisitados pelo Delegado de Polícia em Inquéritos Policiais, e pelo Promotor de Justiça em Procedimentos Investigatórios Criminais, Inquéritos Cíveis Públicos, Procedimentos Administrativos, Procedimentos Preparatórios, Notícias de Fato ou Notícias de Crime”. Em decisão dividida, desempatada pelo voto da Ministra que presidiu o julgamento, a Corte considerou que os dados cadastrais não constituem “dados sigilosos e sujeitos a controle jurisdicional, e tampouco de dados sensíveis, sendo que, por expressa previsão legal, são protegidos de maneira mais branda em relação aos demais dados pessoais” e que “a legislação nacional apresenta formas de garantir a proteção dos dados cadastrais e de evitar eventual abuso no seu acesso e tratamento”, pois “a solicitação de acesso aos dados cadastrais exige prévio procedimento em andamento (cível, administrativo ou criminal) e idônea e expressa motivação pelo órgão competente, sendo desprovida a autorização pelo Judiciário nessa hipótese.” (STJ, Recurso Especial n. 1.955.981-GO, Rel. Min. Nancy Andrighi, julgamento em 05 set. 2024).

tratamento de dados pessoais, tais como o enquadramento nas bases legais (art. 7º e 11), respeito aos princípios de proteção de dados (art. 6º), adoção de medidas técnicas e administrativas de segurança (art. 46), atendimento a requerimentos de titulares (art. 18), registro das operações de tratamento (art. 37), avaliação de riscos e implementação de medidas de mitigação (art. 38), etc.

Além disso, por disposição expressa da LGPD (art. 4º, III), operações de tratamento de dados pessoais realizados para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais estão fora de seu âmbito de aplicação. O tratamento de dados pessoais realizados nessas atividades "será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei" (LGPD, art. 4º, §1º). O projeto de lei da chamada "LGPD Penal" ainda está em tramitação no Congresso Nacional (PL 1515/2022), inexistindo, atualmente, no Brasil legislação específica sobre o tema.

2.2 Dados de tráfego

Os dados de tráfego são definidos na Convenção de Budapeste como "quaisquer dados de computador referentes a uma comunicação por meio de um sistema informatizado, gerados por um computador que seja parte na cadeia de comunicação, e que indicam sua origem, destino, caminho, hora, data, extensão, duração ou tipo de serviço subordinado" (art. 1, d).

No Marco Civil da Internet, os dados de tráfego abrangem duas espécies: os "registros de conexão" e os "registros de acesso a aplicações de internet". O registro de conexão é definido como "o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados" (art. 5º, VI).³¹ Por sua vez, os registros de acesso a aplicações de internet designam "o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP" (art. 5º, VIII).

31. Definição similar consta na Lei 12.850/2013 para a expressão "dados de conexão" (art. 10, §1º, I).

O MCI prevê como direito do usuário o “não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei” (art. 7º, VII). E mais adiante a lei deixa explícita a necessidade de prévia autorização judicial (art. 10, §1º) para acesso de terceiros tanto a registros de conexão (art. 13, §5º) como a registros de acesso a aplicações de internet (art. 15, §3º). Portanto, a obtenção de dados de tráfego, para quaisquer fins, seja por autoridades públicas ou por particulares, está subordinada à reserva de jurisdição, por força do Marco Civil da Internet.

Os parâmetros legais, a serem apreciados pelo juiz para ordenar aos provedores de conexão ou de aplicações de internet o fornecimento dos dados de tráfego, estão previstos no art. 22 do MCI, a saber: I - fundados indícios da ocorrência do ilícito; II - justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e III - período ao qual se referem os registros.

Conforme tem decidido o Superior Tribunal de Justiça acerca desses parâmetros, *“há diferenciação na proteção dada pela legislação ao conteúdo das comunicações mantidas entre indivíduos e às informações de conexão e de acesso a aplicações da internet, [pois] ao tratar das informações de conexão e de acesso a aplicações de internet, encontram-se na Lei n. 12.965/2014 regras mais claras e menos rígidas”*.³²

De fato, os requisitos previstos no art. 22 do MCI para acesso aos dados de tráfego buscam permitir que seja aferida a aptidão da intervenção para o alcance do objetivo almejado. Ou seja, é exigida uma análise apenas do subprincípio da adequação, não se avançando para as demais etapas do princípio da proporcionalidade, como a demonstração da necessidade da medida e ausência de alternativas menos gravosas (subsidiariedade) ou sua limitação à apuração de certa categoria de crimes (proporcionalidade em sentido estrito), como ocorre, por exemplo, na interceptação de comunicações telefônicas e telemáticas, que limita a medida a crimes punidos com reclusão (art. 2º da Lei 9296/1996). O *caput* do art. 22, inclusive, deixa claro que o pedido de acesso a dados de tráfego poderá ser formulado pela “parte interessada [...] com o propósito de formar conjunto probatório em processo judicial cível ou penal”,

32. SUPERIOR TRIBUNAL DE JUSTIÇA, AgRg no AREsp n. 1.789.994/GO, Relator Ministro Joel Ilan Paciornik, julgado em 1 jun. 2021, DJe de 7 jun. 2021.

não limitando, portanto, a legitimidade apenas às autoridades públicas, nem a finalidade somente à persecução criminal.

Nessa linha mais tolerante, o Superior Tribunal de Justiça tem, inclusive, admitido a quebra de sigilo de dados de tráfego em massa para investigação de crimes mais graves, por meio da técnica de busca reversa por localização.³³ Essa técnica consiste em requisitar ao provedor os dados de identificação dos diversos usuários que realizaram conexão ou acesso a aplicações em determinada área geográfica e período de tempo, e, por eliminação, levantar possíveis suspeitos. Uma medida similar é a quebra de sigilo de usuários da internet com base em buscas em sites de pesquisa, como ocorreu nas investigações do homicídio da vereadora Marielle Franco e de seu motorista, Anderson Gomes, em 2018.³⁴ Porém, há sérias críticas à ausência de norma autorizativa para tais medidas genéricas, que poderiam configurar uma forma de *fishing expedition*, e ao tratamento dos dados dos insuspeitos que não interessam à investigação.³⁵

Portanto, embora o acesso a dados de tráfego esteja subordinado à reserva de jurisdição, esse menor grau de rigor para análise do pedido e concessão da medida pelo juiz é proporcional ao nível de afetação da privacidade dos usuários. Na escala de

33. “A determinação judicial de quebra de sigilo de dados informáticos estáticos (registros), relacionados à identificação de usuários que operaram em determinada área geográfica e período de tempo, com fundamentação suficiente, não se mostra desproporcional, nem ofende a proteção constitucional à privacidade e à intimidade.” SUPERIOR TRIBUNAL DE JUSTIÇA, **Jurisprudência em teses**: Marco Civil da Internet II - Lei 12.965/2014. Edição n. 223, Brasília, 11 de outubro de 2023. Disponível em <https://scon.stj.jus.br/SCON/jt/jt.jsp>. Acesso em 07 fev. 2025, p. 5.

34. Nesse caso, atendendo a pedido do Ministério Público, o Tribunal de Justiça do Estado do Rio de Janeiro determinou que o Google informasse os dados de quem pesquisou termos como “Marielle Franco”, “vereadora Marielle” ou o endereço onde a parlamentar esteve antes de ser assassinada, dentro de um período de 96 horas. Essa medida, que foi referendada pelo Superior Tribunal de Justiça, levou à identificação do executor do crime, Ronnie Lessa. O Google recorreu ao Supremo Tribunal Federal e foi reconhecida a repercussão geral do caso (Tema 1.148). O julgamento foi suspenso na sessão de 23/04/2025, com 4 votos, dois pela inconstitucionalidade da medida (ministros Rosa Weber e André Mendonça) e dois pela constitucionalidade (ministros Cristiano Zanin e Alexandre de Moraes).

35. ESTELLITA, Heloisa; GLEIZER, Montenegro. *A investigação penal de insuspeitos*: STJ fere direitos ao exigir coleta massiva de dados. 2020. Disponível em: <https://www1.folha.uol.com.br/opiniao/2020/09/a-investigacao-penal-de-insuspeitos.shtml>. Acesso em: 20 fev. 2025.

ônus aos direitos fundamentais, os dados de tráfego estão em um patamar intermediário, entre os dados cadastrais e os dados de conteúdo, pois revelam aspectos relevantes da vida privada e da intimidade do indivíduo, que permitem inferências de hábitos e perfis dos titulares, mas de forma limitada.

2.3 Dados de conteúdo

Os dados de conteúdo são “*as próprias informações transmitidas durante o processo de telecomunicação*”,³⁶ tais como áudios, vídeos, mensagens de texto e arquivos transmitidos por meio de aplicações de correio eletrônico e de mensagens instantâneas, além de outras aplicações que permitem o envio e recebimento de informações.

Esses dados podem alcançar os espaços mais recônditos da intimidade de alguém, ainda mais com a popularização do *smartphone*, que é usado para múltiplas atividades diárias, dos mais variados campos da vida, representando uma verdadeira extensão da personalidade de seu dono.³⁷ Portanto, é esperado que os dados de conteúdo tenham um maior grau de proteção, proporcional ao nível de afetação que uma intervenção nesses dados pode implicar para os direitos fundamentais do titular.

Diferentemente das categorias de dados anteriores, que encontram respaldo constitucional apenas nos direitos à privacidade e à proteção de dados pessoais (art. 5º, X e LXXIX), por princípio os dados de conteúdo estariam amparados em dispositivo constitucional próprio sobre a inviolabilidade do sigilo das comunicações (art. 5º, XII), que condiciona a restrição a tal direito à prévia autorização judicial, “nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou

36. GLEIZER, Orlandino. A proteção de dados por duas portas nas intervenções informacionais. *Revista de Estudos Criminais*, v. 19, n. 79, 2020, p. 214.

37. Dennys Antonialli e Jacqueline de Souza Abreu destacam que “os telefones celulares, de propriedade da grande maioria dos cidadãos brasileiros, são hoje um tesouro de informações de comunicação e, portanto, de evidências valiosas para agentes de segurança pública” e que, “embora a ‘revolução do smartphone’ represente um marco em termos de acesso ao conhecimento e às comunicações no Brasil, também expõe os cidadãos brasileiros - usuários de smartphones - a uma vigilância maior e mais invasiva.” ABREU, Jaqueline; ANTONIALLI, Dennys. *O conto do baú do tesouro: a expansão da vigilância pela evolução e popularização de celulares no Brasil*. V Simpósio LAVITS, 2017. Disponível em <https://lavits.org/wp-content/uploads/2018/04/33-Jacqueline-de-Souza-Abreu-e-Dennys-Antonialli.pdf>. Acesso em 08 fev. 2025.

instrução processual penal”.³⁸

Entretanto, como explica Jaqueline Abreu, “há anos prevalece no STF a noção de que apenas o ‘processo de comunicar’ é protegido pelo art. 5º, XII, CF/88”, e não o conteúdo comunicado (“dados em si”), tendo sido estabelecida, assim, uma distinção entre “dados em fluxo” e “dados estáticos”.³⁹ Segundo essa lógica, os parâmetros do inciso XII do art. 5º da Constituição para análise da legitimidade da intervenção no direito fundamental só se aplicariam para a interceptação das comunicações em tráfego, enquanto os dados de conteúdo das comunicações armazenadas permaneceriam apenas sob a abrangência das cláusulas gerais dos direitos à privacidade e à proteção de dados pessoais (art. 5º, X e LXXIX, da Constituição).

38. Embora uma interpretação literal do texto do inciso XII (“salvo, no último caso”) sugira que a flexibilização do sigilo seria admitida apenas para as comunicações telefônicas e que as demais formas de comunicação seriam absolutamente invioláveis, “diante do inevitável avanço da tecnologia” prevaleceu na doutrina e na jurisprudência a tese de que “o texto constitucional teria separado as formas de comunicação em dois blocos (comunicação postal e telegráfica, de um lado, e comunicação de dados e telefônica, de outro), de modo que a exceção constitucional seria aplicável ao último, ou seja, às comunicações de dados e telefônicas.” QUITO, Carina. As quebras de sigilo telemático no processo penal e o paradoxo do acesso irrestrito às comunicações armazenadas. In: WOLKART, Erik Navarro et al. (coord.). *Direito, processo e tecnologia*. 2. ed. São Paulo: Thomson Reuters Brasil, 2021, p. 167. Atualmente, o Supremo Tribunal Federal já admite, inclusive, a flexibilização do sigilo postal, conforme entendimento adotado no Tema 1041, em repercussão geral: “(1) Sem autorização judicial ou fora das hipóteses legais, é ilícita a prova obtida mediante abertura de carta, telegrama, pacote ou meio análogo, salvo se ocorrida em estabelecimento penitenciário, quando houver fundados indícios da prática de atividades ilícitas; (2) Em relação a abertura de encomenda postada nos Correios, a prova obtida somente será lícita quando houver fundados indícios da prática de atividade ilícita, formalizando-se as providências adotadas para fins de controle administrativo ou judicial”. SUPREMO TRIBUNAL FEDERAL, Recurso Extraordinário 1116949, Relator(a): Min. Edson Fachin, Julgamento: 30 nov. 2023, Publicação: 24 mai. 2024.

39. A autora analisa a evolução desse entendimento do STF, a partir de quatro precedentes mais relevantes, entre 1994 e 2012, com destaque para o julgamento do Recurso Extraordinário 418.416, de 2006, relatado pelo Min. Sepúlveda Pertence, em que a tese acabou consolidada, inspirada em artigo publicado em 1993 por Tércio Sampaio Ferraz Jr., citado anteriormente. ABREU, Jacqueline de Souza. “Comunicação de dados, não dados em si: origens e problemas do atual paradigma de proteção constitucional do sigilo de dados”. *Revista de Investigações Constitucionais*. Curitiba, vol. 11, n. 1, jan./abr. 2024, p. 6-13.

No plano infraconstitucional, o Marco Civil da Internet prevê como direitos do usuário (art. 7º) a inviolabilidade, o sigilo e a reserva de jurisdição para os dados de conteúdo, tanto para o “fluxo de suas comunicações pela internet” (inciso II) como para “suas comunicações privadas armazenadas” (inciso III). Portanto, para acesso a dados de conteúdo das comunicações, em fluxo ou estáticos, é sempre necessária prévia autorização judicial, como sintetiza o §2º do art. 10 do MCI: “§2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º”.⁴⁰

No caso das comunicações em fluxo, o acesso aos dados de conteúdo se subordina ao disposto na Lei 9296/1996, que regulamenta a interceptação telefônica e telemática. Segundo a lei, em resumo, a interceptação é restrita à finalidade de persecução criminal de infração penal punida com pena de reclusão e depende de decisão judicial fundamentada, a partir de requerimento da autoridade policial ou do Ministério Público, em que se deve demonstrar a existência de indícios razoáveis da autoria delitiva e a necessidade da medida para apuração da infração penal (inexistência de outros meios disponíveis para obtenção da prova), estendendo-se por períodos renováveis de 15 dias (art. 1º a 5º).

40. Após o advento do MCI, a jurisprudência do Superior Tribunal de Justiça consolidou-se no sentido de que os dados armazenados em dispositivos apreendidos, seja durante o flagrante de crime, seja em cumprimento de mandado de busca e apreensão, só podem ser acessados pelas autoridades após autorização judicial, com justificativa quanto à necessidade e abrangência da medida. Também se considera o acesso válido quando há a concordância do titular, porém, nesse caso, cabe à autoridade o ônus da prova de que esse consentimento ocorreu de forma livre, sem coação, por exemplo, por meio de testemunhas ou registro audiovisual. COSTA, Gilberto Ferreira, *Regulação e governança de internet no Brasil: a jurisprudência do Superior Tribunal de Justiça sobre o Marco Civil da Internet*, 2024. Dissertação de Mestrado: Brasília: UNB, 2024, p. 69-74. No Supremo Tribunal Federal, a questão é objeto do tema 977 de repercussão geral (ARE 1042075), cujo julgamento, na presente data, ainda está pendente de conclusão, mas já há a seguinte proposta de tese: “1. O acesso a registro telefônico, agenda de contatos e demais dados contidos em aparelhos celulares apreendidos no local do crime atribuído ao acusado depende de prévia decisão judicial que justifique, com base em elementos concretos, a necessidade e a adequação da medida e delimite a sua abrangência à luz dos direitos fundamentais à intimidade, à privacidade, ao sigilo das comunicações e à proteção dos dados pessoais, inclusive nos meios digitais (CF, art. 5º, X, XII e LXXIX).”

Já para as comunicações privadas armazenadas não existem quaisquer parâmetros específicos previstos na legislação para orientar a análise pelo juiz acerca da legitimidade da intervenção. Não há na legislação limitação temporal,⁴¹ restrição das finalidades para as quais a medida é cabível, nem exigência de demonstração da adequação e necessidade da providência ou de delimitação de sua abrangência. A análise fica ao alvedrio de cada juiz, conforme sua apreciação pessoal do princípio da proporcionalidade como mecanismo instrumental para aferir a legitimidade de restrições a direitos fundamentais. Essa situação, como bem aponta Carina Quito, “*cria o seguinte paradoxo: enquanto em tráfego, as mensagens trocadas são protegidas com rigor; no instante seguinte ao seu armazenamento (...), o rigor desaparece, viabilizando acesso praticamente irrestrito aos registros de conteúdos comunicados, desde que haja, para tanto, autorização judicial.*”⁴²

De fato, esse teste binário “dados dinâmicos x dados estáticos”, criado a partir da jurisprudência dos Tribunais Superiores, para além de anacrônico,⁴³ produz uma intolerável insegurança jurídica, tanto para a pessoa afetada pela medida, como para os órgãos de investigação e persecução penal. Há, portanto, necessidade de revisão da matéria, seja mediante a mudança do entendimento dos Tribunais Superiores ou por regulamentação específica de parâmetros para o acesso às comunicações privadas armazenadas.

41. “Nas investigações criminais, o acesso a dados telemáticos armazenados não exige delimitação temporal.” Superior Tribunal de Justiça, *Jurisprudência em teses*: Marco Civil da Internet II - Lei 12.965/2014. Edição n. 223, Brasília, 11 de outubro de 2023. Disponível em <https://scon.stj.jus.br/SCON/jt/jt.jsp>. Acesso em 07 fev. 2025, p. 5.

42. QUITO, Carina. As quebras de sigilo telemático no processo penal e o paradoxo do acesso irrestrito às comunicações armazenadas. In: WOLKART, Erik Navarro et al. (coord.). *Direito, processo e tecnologia*. 2. ed. São Paulo: Thomson Reuters Brasil, 2021, p. 179-180.

43. No atual estágio tecnológico, em que o tráfego de dados ocorre de maneira instantânea e o resultado das comunicações permanece armazenado virtualmente, não há diferenciação entre dados em trânsito e armazenados. SIDI, Ricardo. *A interceptação das comunicações telemáticas no processo penal*. Belo Horizonte: Editora D’Plácido, 2016, p. 301-302. FERRAZ JR, Tércio Sampaio Ferraz. Sigilo de dados: o direito à privacidade e os limites do poder do Estado: 25 anos depois, p. 20-40 e MARANHÃO, Juliano. O que é dado não é comunicado, p. 44-55, In: ABREU, Jacqueline de Souza; ANTONIALLI, Dennys (eds.). *Direitos Fundamentais e Processo Penal na Era Digital: Doutrina e Prática em Debate*. Vol. I. São Paulo. InternetLab, 2018.

Por fim, há diversos outros dados de conteúdo que não são propriamente comunicações humanas, pois não foram transmitidas de um indivíduo a outro, como listas de contatos, extratos de mensagens, agendas de compromissos, participação em grupos e redes sociais, fotos, arquivos de texto, vídeo e áudio, planilhas, dados de localização e de deslocamentos feitos pelos usuários, histórico de navegação, histórico de pesquisas, lista de aplicativos baixados, informações sobre compras online, etc, estejam eles armazenados em dispositivos físicos ou nos servidores dos provedores de aplicação.⁴⁴

Todos esses dados pessoais, que também revelam aspectos relevantes da vida privada e intimidade de seus titulares, estão inequivocamente abrangidos pela garantia geral dos direitos à privacidade e à proteção de dados pessoais (art. 5º, X e LXXIX, da Constituição). Porém, diferentemente das “comunicações privadas armazenadas”, resguardadas, ao menos, pela cláusula de reserva de jurisdição estabelecida nos art. 7º, III, e 10, §2º do MCI, não há na legislação qualquer disposição específica a respeito desses dados de conteúdo diversos da comunicação.⁴⁵

3. CONSERVAÇÃO DOS DADOS NAS COMUNICAÇÕES PELA INTERNET

Uma regra básica do regime de proteção de dados pessoais, em consonância com os princípios da finalidade, adequação e necessidade (LGPD, art. 6º, I, II e III), é a obrigação do controlador eliminar os dados após o término do seu tratamento, especialmente quando se verificar que “a finalidade foi alcançada (...) ou que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada”, ou, ainda, a pedido do titular quando o tratamento tiver por base legal o seu consentimento (art. 15, I e III, 16 e 18, VI, da LGPD).⁴⁶

44. QUITO, Carina. As quebras de sigilo telemático no processo penal e o paradoxo do acesso irrestrito às comunicações armazenadas. In: WOLKART, Erik Navarro et al. (coord.). *Direito, processo e tecnologia*. 2. ed. São Paulo: Thomson Reuters Brasil, 2021, p. 171.

45. Segundo Carina Quito, na prática judiciária, para acesso das autoridades de persecução criminal a esses dados é comum que se utilize como fundamento as disposições que tratam da busca e apreensão (art. 240 e seguintes do CPP). QUITO, Carina, id., p. 172.

46. Seja por ausência de políticas claras sobre prazos para eliminação, seja pela não incorporação, por

De forma semelhante, o MCI prevê como direito do usuário a “exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes” (art. 7º, X). Porém, tanto a LGPD como o MCI ressaltam que, mesmo após o término do tratamento, os dados podem ser conservados para “cumprimento de obrigação legal ou regulatória pelo controlador” (LGPD, art. 16, I) e em razão das regras sobre “guarda obrigatória de registros” (MCI, art. 7º, X).

Assim, a conservação de dados dos usuários pelos provedores visa cumprir dois tipos de obrigações: (a) o dever geral de guarda dos dados por um certo período de tempo (*data retention*); e (b) o dever de atendimento a requisições de autoridades para preservação de dados específicos até que seja obtida autorização judicial para o acesso (*data preservation*).

3.1 Guarda de dados (*data retention*)

A guarda ou retenção de dados (*data retention*) consiste na obrigação dos provedores de coletar e armazenar, de forma geral e indiscriminada, dados dos usuários de seus serviços por um determinado período de tempo.

Embora justificada principalmente por razões de segurança pública, prevenção, investigação e repressão a crimes, a retenção massiva e indiscriminada de dados, em alguma medida, impacta os direitos à presunção de inocência e à privacidade dos usuários, especialmente quanto maior a quantidade de dados coletados e o tempo de retenção exigido.⁴⁷

padrão (*privacy by-default*), dessas políticas nas funcionalidades das aplicações, ou mesmo por desconhecimento ou desídia dos usuários quanto às configurações de privacidade das aplicações, é bastante comum que dados pessoais coletados massivamente na interação cotidiana do usuário com a tecnologia e em suas comunicações pela internet permaneçam armazenados indefinidamente em dispositivos físicos ou nos servidores dos provedores, o que representa um sério risco à privacidade dos usuários.

47. A propósito, em 2014, o Tribunal de Justiça da União Europeia decidiu pela anulação da Diretiva europeia relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrônicas (Diretiva 2006/24/EC), por considerar que não foi implementada uma adequada ponderação entre o dever de segurança do Estado e o direito à privacidade dos

No Brasil, a obrigação legal de guarda está restrita aos dados de tráfego, não alcançando dados cadastrais,⁴⁸ nem muito menos dados de conteúdo.⁴⁹ Segundo o art. 13 do MCI, os registros de conexão deverão ser mantidos pelo período de 1 (um) ano pelo administrador de sistema autônomo de provisão de conexão à internet. Já os registros de acesso a aplicações de internet deverão ser mantidos pelo provedor pelo prazo de 6 (seis) meses, conforme o art. 15 do MCI. O descumprimento da obrigação de guarda pelos provedores poderá ensejar a aplicação das sanções previstas no art. 12 do MCI.

Nos últimos anos chegou ao Superior Tribunal de Justiça a discussão se a obrigação de guarda dos provedores abrange também os dados da porta lógica de origem associada aos endereços do tipo IPv4, modelo de endereçamento de conexão que

indivíduos. UNIÃO EUROPEIA. Tribunal de Justiça (Grande Seção). *Acórdão de 8 de abril de 2014, Processos apensos C-293/12 e C-594/12*. Disponível em: <https://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&do->

[clang=pt&mode=lst&dir=&occ=first&part=1&cid=654354](https://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&do-clang=pt&mode=lst&dir=&occ=first&part=1&cid=654354). Acesso em: 9 fev. 2025. Na doutrina, vide SILVEIRA, Alessandra; FREITAS, Pedro Miguel. Implicações da declaração de invalidade da Diretiva 2006/24 na conservação de dados (“metadados”) nos Estados-Membros da UE: uma leitura jusfundamental. *Journal of Law and Regulation*, v. 3, n. 1, p. 281–302, 2017; e ABREU, Jaqueline. Guarda Obrigatória de Registros de Telecomunicações no Brasil: sobre as origens da retenção de dados e as perspectivas para direitos fundamentais, *Nuevos Paradigmas de la Vigilancia*?, Disponível em: <http://lavits.org/wpcontent/uploads/2017/08/P5_De_Souza_Abreu.pdf>. Acesso em 02 mar. 2025.

48. Apesar de ser comum a prática dos provedores de armazenar dados básicos de seus usuários para outras finalidades (cobrança, comunicação, publicidade, etc), não há obrigação legal de guarda de dados cadastrais, como se nota pelo art. 11, §1º, do Decreto 8771/2016. Por outro lado, no caso “La Quadrature du Net”, o Tribunal de Justiça da União Europeia considerou que os Estados Membros podem impor aos provedores obrigações de guarda de dados relativos à identidade civil dos usuários de seus serviços “para efeitos de prevenção, investigação, deteção e repressão de infrações penais, assim como da salvaguarda da segurança pública.” UNIÃO EUROPEIA. Tribunal de Justiça (Grande Seção). *Acórdão de 6 de outubro de 2020, Processos apensos C511/18, C512/18 e C520/18*. Disponível em: <https://curia.europa.eu/juris/document/document.jsf?sessionid=EBF20EE5EAFBB229F2CFDFB00F9E9B2A?text=&docid=232084&pageIndex=0&do-clang=PT&mode=lst&dir=&occ=first&part=1&cid=632727>. Acesso em: 9 fev. 2025, §159.

49. SUPERIOR TRIBUNAL DE JUSTIÇA, 3ª Turma, *REsp 1885201/SP*, Rel. Ministra Nancy Andrighi, julgado em 23/11/2021, DJe 25/11/2021; *AgRg no RMS 56496 / RS*, Rel. Min. Sebastião Reis Júnior, julgado em 17/04/2018, DJe 30/04/2018.

permite o acesso simultâneo de vários usuários com o mesmo IP, atualmente em processo de transição para o modelo IPv6.

Embora os dados da porta lógica não integrem as definições do MCI para registro de conexão (art. 5º, VI) e registro de acesso a aplicações de internet (art. 5º, VIII), tem prevalecido no STJ uma interpretação extensiva do MCI⁵⁰ no sentido de que “os provedores de acesso e os de aplicação têm o dever de guarda e armazenamento dos dados referentes ao IP e à porta lógica de origem, para possibilitar a identificação de usuários da internet que tenham cometido atos ilícitos de qualquer natureza praticados no âmbito virtual”.⁵¹

3.2 Preservação de dados (*data preservation*)

A preservação de dados (*data preservation*) é uma medida administrativa, de natureza pré-cautelar, destinada a evitar o perecimento da prova, em razão da volatilidade dos dados digitais, e assegurar sua disponibilidade no momento em que for concedido o acesso aos dados.⁵²

De acordo com o MCI, a autoridade policial ou administrativa ou o Ministério

50. Essa interpretação extensiva tem sido alvo de críticas da doutrina. ANTONIALLI, Dennys; CRUZ, Francisco Brito; FRAGOSO, Nathalie. *O Marco Civil da Internet e o dilema da ‘porta lógica’*. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/o-marco-civil-da-internet-e-o-dilema-da-porta-logica-22082019>. Acesso em: 9 fev. 2025. RAMOS, Pedro; MONTEIRO, Renato. *Armazenamento de portas lógicas à luz do MCI*. Disponível em: https://baptistaluz.com.br/institucional/adiscussao-sobre-armazenamento-de-portas-logicas-a-luz-do-mci/#_ftnref5. Acesso em: 9 fev. 2025.

51. SUPERIOR TRIBUNAL DE JUSTIÇA, *Jurisprudência em teses*: Marco Civil da Internet II - Lei 12.965/2014. Edição n. 223, Brasília, 11 de outubro de 2023. Disponível em <https://scon.stj.jus.br/SCON/jt/jt.jsp>. Acesso em 07 fev. 2025, p. 2.

52. “Assim, tal como ocorre com as providências do inciso I do art. 6º do CPP, a preservação dos dados a pedido da Polícia ou do MP tem função acautelatória, *ad perpetuam rei memoriam*, uma vez que dados de tráfego de Internet e de acesso a aplicações são usualmente apagados ou anonimizados quando cumprem suas finalidades técnico-operacionais, no provedor, ou quando findo o prazo de guarda.” ARAS, Vladimir. O congelamento de dados informáticos para fins de prova no processo. *Delictae Revista de Estudos Interdisciplinares sobre o Delito*_8, n.15, 2023. Disponível em <https://delictae.com.br/index.php/revista/article/view/225>. Acesso em 07 fev. 2025, p. 199-201.

Público poderão requerer cautelarmente ao provedor que os registros de conexão (art. 13, §2º) e/ou os registros de acesso a aplicações de internet (art. 15, §2º) sejam preservados, inclusive por prazo superior ao prazo legal de guarda desses dados.⁵³ Uma vez preservados os dados, “a autoridade requerente terá o prazo de 60 (sessenta) dias, contados a partir do requerimento, para ingressar com o pedido de autorização judicial de acesso aos registros” (art. 13, §3º). A medida “perderá sua eficácia caso o pedido de autorização judicial seja indeferido ou não tenha sido protocolado no prazo previsto” (art. 13, §4º).

Embora a preservação dos dados, como mera medida acautelatória, não esteja sujeita à reserva de jurisdição, bastando a requisição da autoridade, o acesso aos dados continua dependendo de autorização judicial, o que vale tanto para dados de tráfego (MCI, art. 10, §1º, art. 13, §5º, art. 15, §3º e art. 22), como para dados de conteúdo (MCI, art. 7º, II e III, art. 10, §2º).

Na Convenção de Budapeste, a medida está prevista nos art. 16 e 17, sob o título de “preservação expedita de dados de computador”, abrangendo não só dados de tráfego como também os dados de conteúdo. Segundo o texto da Convenção, a “ordem” de preservação, cabível “especialmente quando haja razões para admitir que os dados de computador estão particularmente sujeitos a perda ou modificação” (art. 16.1), perdurará por “até o máximo de 90 dias, a fim de permitir à autoridade competente buscar sua revelação” (art. 16.2).

Decisão polêmica acerca da preservação de dados foi tomada pela 2ª Turma do Supremo Tribunal Federal, no julgamento do Agravo Regimental no Habeas Corpus n. 222141/PR. Nesse caso, envolvendo a investigação de um esquema de organização criminosa e fraude a licitações com participação de funcionários do Detran/PR, o Ministério Público do Paraná havia requisitado diretamente à Apple a preservação de dados telemáticos, incluindo dados de conteúdo, como “histórico de pesquisa, todo conteúdo de e-mail e iMessages, fotos, contatos e históricos de localização”. Uma semana depois da requisição de preservação dos dados, o *Parquet* requereu à

53. Embora a lei utilize o termo “requerer”, o sentido é de “requisitar”, pois se trata de uma ordem, que o provedor está obrigado a cumprir, conforme reconheceu o Superior Tribunal de Justiça no julgamento do HC 626983/PR, Rel. Des. Olindo Menezes, julgado em 08 fev. 2022, DJe 22 fev. 2022. É o que se depreende também do disposto no art. 16.2 da Convenção de Budapeste.

Justiça autorização para obtenção dos dados preservados (quebra de sigilo telemático), tendo o pedido sido deferido pelo juízo e, só então, os dados foram acessados.

Ao apreciar o Habeas Corpus impetrado contra decisão do Superior Tribunal de Justiça (HC 626.983/PR), que havia negado o pedido de suspensão do trâmite da ação penal, o Ministro Ricardo Lewandowski, do STF, em decisão monocrática, decidiu por conceder a ordem, *“a fim de declarar nulos os elementos de prova angariados em desfavor da paciente a partir do congelamento prévio, sem autorização judicial, do conteúdo de suas contas eletrônicas, bem como de todos os demais que dele decorrem”*.⁵⁴ Segundo o ministro relator, a preservação dos dados implicaria seu “congelamento”, o que retiraria *“do seu legítimo proprietário o direito de dispor do conteúdo dos seus dados para quaisquer fins”*. Além disso, o MCI restringiria a medida de preservação por requisição direta das autoridades tão somente aos dados de tráfego, não abarcando dados de conteúdo, que estariam, portanto, sujeitos à cláusula de reserva de jurisdição, seja para o acesso ou apenas para a preservação.

Como essa decisão é anterior à incorporação da Convenção de Budapeste no ordenamento brasileiro, acreditava-se que ela poderia ser revista por ocasião da apreciação pela Turma dos recursos interpostos pelo Ministério Público, nos quais arguiu-se, inclusive, a aplicação imediata das disposições da Convenção, que passou a vigor internamente em 13/04/2023. Porém, na sessão de 6 de fevereiro de 2024, por maioria de votos, a decisão monocrática acabou mantida, sob o entendimento de que o MCI *“não autoriza ao Ministério Público, sem prévia autorização judicial, o requerimento de preservação de dados pessoais e do conteúdo de comunicações privadas”* e que *“o mero congelamento de dados sem autorização judicial e fora das hipóteses legais afronta a tutela da privacidade”*.⁵⁵

A aludida decisão é passível de crítica e o entendimento adotado na ocasião pode

54. SUPREMO TRIBUNAL FEDERAL, HC 222141, decisão monocrática do Ministro Ricardo Lewandowski, 1/12/2022. Disponível em <https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=498969&ori=1>. Acesso em 24 fev. 2025.

55. Além do Ministro Ricardo Lewandowski, votaram pela denegação dos recursos do Ministério Público os Ministros Gilmar Mendes e Nunes Marques, vencidos os Ministros Edson Fachin e André Mendonça. SUPREMO TRIBUNAL FEDERAL, Ag. Reg. no HC 222141, redator Min. Gilmar Mendes, julgamento em 06/02/2024, publicado no DJE 03/04/2024. Contra o acórdão, foram opostos embargos declaratórios, ainda pendentes de julgamento, na presente data.

voltar a ser examinado,⁵⁶ seja porque a Convenção de Budapeste não restringe a medida de preservação somente a dados de tráfego, contemplando quaisquer dados de computador,⁵⁷ conforme dicção do art. 16.1, seja porque a preservação de dados, como medida meramente acautelatória, apenas cria um registro (uma fotografia) dos dados disponíveis em determinado momento (cuja revelação dependerá de ordem judicial), não subtraindo do titular a disponibilidade sobre os dados.⁵⁸

56. Além disso, como destacado pelo Ministro André Mendonça no voto vencido, “o pedido de preservação de dados não se apresenta como um dos meios de obtenção ou produção de prova [...] e não produz qualquer resultado probatório”. Assim, como “a produção de prova somente ocorre após o afastamento do sigilo por ordem judicial, não [existe] nexo de causalidade entre a atividade persecutória apontada como ilegítima e a introdução do material probatório nos autos.” SUPREMO TRIBUNAL FEDERAL, Ag. Reg. no HC 222141, redator Min. Gilmar Mendes, julgamento em 06 fev. 2024, publicado no DJE 03 abr. 2024, p. 18.

57. Segundo ARAS: “De fato, ao se referir, no seu art. 16, à preservação expedita de dados de computador, a Convenção 185 abarca todas as categorias de dados armazenados (*stored data*), inclusive os dados de conteúdo e os dados de tráfego. Deste modo, os Estados Partes ficam obrigados – e o Brasil, entre eles, desde a vigência do tratado – a adotar providências legislativas para dar lugar a medidas cautelares e de obtenção de provas digitais. (...) Com exceção das normas de direito penal – que dependem de lei em função do princípio da legalidade penal estrita –, as normas conceituais e as de natureza processual da Convenção de Budapeste têm aplicação instantânea, nos termos do art. 1º, inciso I do CPP – que prevê o princípio da especialidade –, e do art. 2º do CPP, que institui o princípio do efeito imediato. Desta maneira, desde 13 de abril de 2023, diante da mora legislativa, a Polícia Judiciária e o Ministério Público podem invocar os arts. 16 e 17 da Convenção de Budapeste para as medidas de preservação expedita de dados de computador (inclusive *traffic data* e *content data*), pelo prazo máximo de sessenta dias, independentemente de ordem judicial.” ARAS, Vladimir. O congelamento de dados informáticos para fins de prova no processo. *Delictae Revista de Estudos Interdisciplinares sobre o Delito*_ 8, n.15, 2023. Disponível em <https://delictae.com.br/index.php/revista/article/view/225>. Acesso em 07 fev. 2025, p. 210-211.

58. O relatório explicativo da Convenção de Budapeste deixa claro do que a preservação dos dados não implica torná-los indisponíveis ao titular: “*Preservation requires that data, which already exists in a stored form, be protected from anything that would cause its current quality or condition to change or deteriorate. It requires that it be kept safe from modification, deterioration or deletion. Preservation does not necessarily mean that the data be “frozen” (i.e. rendered inaccessible) and that it, or copies thereof, cannot be used by legitimate users. The person to whom the order is addressed may, depending on the exact specifications of the order, still access the data.*” COUNCIL OF EUROPE. *Explanatory Report to the Convention on Cybercrime*. Budapest, 23 XI 2001. Disponível em: <https://rm.coe.int/16800cce5b>. Acesso em: 02 mar. 2025, p. 26.

4. CONCLUSÃO

O Marco Civil da Internet trouxe inegáveis avanços para a conformação do regime das provas digitais no ordenamento jurídico brasileiro, explicitando certas regras para equilibrar os direitos individuais à privacidade e à proteção de dados pessoais com o direito coletivo à segurança pública, voltado à prevenção e investigação de infrações penais e, em última instância, à própria concretização de direitos fundamentais (vedação de proteção deficiente).

Assim, considerando os entendimentos consolidados na jurisprudência ao longo de uma década desde a instituição do MCI, estão razoavelmente bem estabelecidas as normas sobre os limites temporais e materiais para guarda de dados pelos provedores, a abrangência e legitimidade para acesso a dados cadastrais pelas autoridades públicas, os requisitos procedimentais para preservação e os parâmetros para acesso a dados de tráfego e a sujeição à cláusula de reserva de jurisdição para acesso a dados de conteúdo das comunicações armazenadas.

Por outro lado, alguns aspectos das provas digitais ainda carecem de uma regulamentação apropriada.

Em certos casos, a legislação é completamente omissa em relação ao tema, demandando construções casuísticas a partir das cláusulas constitucionais do direito à privacidade e à proteção de dados pessoais, como se dá em relação ao acesso a dados de conteúdo armazenados diversos das comunicações, bem como na aplicação de técnicas mais invasivas, como a vigilância algorítmica, o *hackeamento* estatal e a infiltração por *malware*, que tendem a se tornar cada vez mais comuns e ampliar espaços para abusos.

Em outros casos, as normas atuais são limitadas e insuficientes. Essa é a hipótese do acesso a dados de conteúdo das comunicações armazenadas, que, embora sujeito à cláusula da reserva de jurisdição, não está vinculado a parâmetros claros de proporcionalidade para aferir a legitimidade da intervenção, como se dá, atualmente, em relação aos requisitos para acesso a dados de tráfego e para interceptação das comunicações em fluxo.

Da mesma forma, embora a jurisprudência venha admitindo a quebra de sigilo de dados de tráfego em massa, para uso da técnica de busca por localização reversa, seria

importante uma regulamentação mais minuciosa dessa situação, tanto em relação a parâmetros de proporcionalidade para emprego dessa medida altamente invasiva, como para disciplinar o tratamento dos dados dos terceiros insuspeitos afetados pela intervenção.

Outra questão que demanda uma atuação do legislador, em prol da segurança jurídica e para atendimento do compromisso assumido pelo Brasil por força da Convenção de Budapeste, é a preservação de dados de conteúdo a partir da requisição direta das autoridades investigativas, até que se obtenha decisão judicial para viabilizar o acesso ao material, a fim de evitar que evidências relevantes para o esclarecimento de crimes sejam destruídas ou se percam, ou, ainda, que os elementos obtidos sejam declarados ilícitos.

Enfim, com o avanço da tecnologia as provas digitais têm se tornado uma fonte essencial para a apuração de atos ilícitos e o direito brasileiro precisa prover normas adequadas, claras e completas acerca do tema. Apesar dos avanços trazidos pelo Marco Civil da Internet, ainda há espaços importantes que exigem aperfeiçoamento legislativo para garantir maior segurança jurídica e proteção dos direitos fundamentais no ambiente digital.

REFERÊNCIAS

- ABREU, Jaqueline. Guarda Obrigatória de Registros de Telecomunicações no Brasil: sobre as origens da retenção de dados e as perspectivas para direitos fundamentais, *Nuevos Paradigmas de la Vigilancia*?, Disponível em: <http://lavits.org/wpcontent/uploads/2017/08/P5_De_Souza_Abreu.pdf>. Acesso em 02 mar. 2025.
- ABREU, Jaqueline. “Comunicação de dados, não dados em si: origens e problemas do atual paradigma de proteção constitucional do sigilo de dados”. *Revista de Investigações Constitucionais*. Curitiba, vol. 11, n. 1, jan./abr. 2024.
- ABREU, Jaqueline; ANTONIALLI, Dennys. *O conto do baú do tesouro: a expansão da vigilância pela evolução e popularização de celulares no Brasil*. V Simpósio LAVITS, 2017. Disponível em <https://lavits.org/wp-content/uploads/2018/04/33-Jacqueline-de-Souza-Abreu-e-Dennys-Antonialli.pdf>. Acesso em 08 fev. 2025.
- ANTONIALLI, Dennys; CRUZ, Francisco Brito; FRAGOSO, Nathalie. *O Marco Civil da Internet e o dilema da ‘porta lógica’*. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/o-marco-civil-da-internet-e-o-dilema-da-porta-logica-22082019>. Acesso em: 9 fev. 2025.
- ARAS, Vladimir. O congelamento de dados informáticos para fins de prova no processo. *Delictae*

- Revista de Estudos Interdisciplinares sobre o Delito_ 8, n.15, 2023. Disponível em <https://delictae.com.br/index.php/revista/article/view/225>. Acesso em 07 fev. 2025.
- BADARÓ, Gustavo. Os standards metodológicos de produção na prova digital e a importância da cadeia de custódia. *Boletim IBCCRIM*, São Paulo, ano 29, n. 343, jun. 2021.
- BARROSO, Luís Roberto. *Curso de Direito Constitucional contemporâneo*. 8ª ed., São Paulo: Saraiva, 2019.
- COSTA, Gilberto Ferreira. *Regulação e governança de internet no Brasil : a jurisprudência do Superior Tribunal de Justiça sobre o Marco Civil da Internet*. Dissertação de mestrado. Brasília: UNB, 2024.
- COUNCIL OF EUROPE. *Explanatory Report to the Convention on Cybercrime*. Budapest, 23 XI 2001. Disponível em: <https://rm.coe.int/16800cce5b>. Acesso em: 02 mar. 2025.
- ESTELLITA, Heloísa; GLEIZER, Montenegro. *A investigação penal de insuspeitos*: STJ fere direitos ao exigir coleta massiva de dados. 2020. Disponível em: <https://www1.folha.uol.com.br/opiniao/2020/09/a-investigacao-penal-de-insuspeitos.shtml>. Acesso em: 20 fev. 2025.
- FERRAZ JÚNIOR, Tércio Sampaio. *Sigilo de dados*: o direito à privacidade e os limites à função fiscalizadora do Estado. *Revista da Faculdade de Direito da Universidade de São Paulo*. São Paulo, v. 88, jan./dez. 1993.
- FERRAZ JÚNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites do poder do Estado: 25 anos depois, p. 20-40, in ANTONIALLI, Dennys (eds.). *Direitos Fundamentais e Processo Penal na Era Digital*: Doutrina e Prática em Debate. Vol. I. São Paulo. InternetLab, 2018.
- GLEIZER; Orlandino. *Busca estatal por informações digitais e intervenções em direitos fundamentais no processo penal*: A 1ª parte da análise sobre quatro casos mencionados em reportagem do JOTA. 2019. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/penal-em-foco/busca-estatal-por-informacoes-digitais-e-intervencoes-em-direitos-fundamentais-no-processo-penal>. Acesso em: 04 fev. 2025.
- GLEIZER; Orlandino. A proteção de dados por duas portas nas intervenções informacionais. *Revista de Estudos Criminais*, v. 19, n. 79, 2020.
- GOMES FILHO, Antonio Magalhães. Notas sobre a terminologia da prova (reflexos no processo penal brasileiro). In: YARSHELL, Flávio Luiz; DE MORAES, Zanoide (Coords.). *Estudos em Homenagem à Professora Ada Pellegrini Grinover*. São Paulo: Editora DPJ, 2005.
- MAGRANI, Eduardo. Threats of the Internet of Things in a techno regulated society: A New Legal Challenge of the Information Revolution. In: *Orbit Journal*. Vol 1. Issue 1. 2017, p. 1-17.
- MARANHÃO, Juliano. O que é dado não é comunicado, p. 44-55, In. ABREU, Jacqueline de Souza; ANTONIALLI, Dennys (eds.). *Direitos Fundamentais e Processo Penal na Era Digital*: Doutrina e Prática em Debate. Vol. I. São Paulo. InternetLab, 2018.
- MEIRA, Silvio. *Sinais do futuro imediato, #1: internet das coisas*. Ikewai, Recife, dez. 2016.
- MEIRA, Silvio. *23 anotações sobre 2023 [x] – 5G & a internet das coisas*. Disponível em:

- <https://silvio.meira.com/silvio/23-anotacoes-sobre-2023-x/>. Acesso em: 03 fev. 2025.
- MELO, Isabella Gabriele Campelo de, *Direito à privacidade na era digital : a vigilância estatal algorítmica da comunicação no sistema europeu de direitos humanos*, Dissertação: Coimbra, 2024
- MENDES, Laura Schertel. O diálogo entre o Marco Civil da Internet e o Código de Defesa do Consumidor. *Revista de Direito do Consumidor*. vol. 106, ano 25, São Paulo: Ed. RT, jul.-ago. 2016.
- QUITO, Carina. As quebras de sigilo telemático no processo penal e o paradoxo do acesso irrestrito às comunicações armazenadas. In: WOLKART, Erik Navarro et al. (coord.). *Direito, processo e tecnologia*. 2. ed. São Paulo: Thomson Reuters Brasil, 2021
- RAMALHO, David Silva. *Métodos ocultos de investigação criminal em ambiente digital*, Coimbra: Almedina, 2017.
- RAMOS, Pedro; MONTEIRO, Renato. *Armazenamento de portas lógicas à luz do MCI*. Disponível em: https://baptistaluz.com.br/institucional/adiscussao-sobre-armazenamento-de-portas-logicas-a-luz-do-mci/#_ftnref5. Acesso em: 9 fev. 2025.
- SAAD, Marta; ROSSI, Helena Costa; PARTATA, Pedro Henrique, A obtenção das provas digitais no processo penal demanda uma disciplina jurídica própria? Uma análise do conceito, das características e das peculiaridades das provas digitais, *Revista Brasileira de Direito Processual Penal*, v. 10, n. 3, 2024.
- SARLET, Ingo Wolfgang. *Proteção de dados pessoais como direito fundamental na Constituição Federal brasileira de 1988*: contributo para a construção de uma dogmática constitucionalmente adequada. *Direitos Fundamentais e Justiça*. Belo Horizonte, v.14, n.42, jan./jun. 2020.
- SIDI, Ricardo. *A interceptação das comunicações telemáticas no processo penal*. Belo Horizonte: Editora D'Plácido, 2016.
- SILVEIRA, Alessandra; FREITAS, Pedro Miguel. Implicações da declaração de invalidade da Diretiva 2006/24 na conservação de dados (“metadados”) nos Estados-Membros da UE: uma leitura jusfundamental. *Journal of Law and Regulation*, v. 3, n. 1, p. 281–302, 2017.
- SMANIO, Gianluca Martins. *Vigilância policial em meio digital: entre o garantismo e a eficiência*. Curitiba: Juruá, 2022, p. 192-193.
- SUPERIOR TRIBUNAL DE JUSTIÇA, *Jurisprudência em teses*: Marco Civil da Internet II - Lei 12.965/2014. Edição n. 223, Brasília, 11 de outubro de 2023. Disponível em <https://scon.stj.jus.br/SCON/jt/jt.jsp>. Acesso em 07 fev. 2025.
- SUPERIOR TRIBUNAL DE JUSTIÇA. *AgRg no AREsp n. 1.789.994/GO*, Relator Ministro Joel Ilan Paciornik, julgado em 1 jun. 2021, DJe de 7 jun. 2021.
- SUPERIOR TRIBUNAL DE JUSTIÇA. *REsp 1885201/SP*, Rel. Ministra Nancy Andriighi, julgado em 23 nov. 2021, DJe 25 nov. 2021.
- SUPERIOR TRIBUNAL DE JUSTIÇA. *AgRg no RMS 56496 / RS*, Rel. Min. Sebastião Reis Júnior, julgado em 17 abr. 2018, DJe 30 abr. 2018.

SUPREMO TRIBUNAL FEDERAL, *Recurso Extraordinário 1116949*, Relator(a): Min. Edson Fachin, Julgamento: 30 nov. 2023, Publicação: 24 mai. 2024.

SUPREMO TRIBUNAL FEDERAL. *HC 222141*, decisão monocrática do Ministro Ricardo Lewandowski, 1 dez. 2022. Disponível em <https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=498969&ori=1>. Acesso em 24 fev. 2025.

SUPREMO TRIBUNAL FEDERAL. *Ag. Reg. no HC 222141*, redator Min. Gilmar Mendes, julgamento em 06 fev. 2024, publicado no DJE 03 abr. 2024.

TILT UOL, *Como agia app espião de Israel que hackeou o WhatsApp de civis sem clicar...* 06/02/2025, Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2025/02/06/como-agia-app-espiao-de-israel-que-hackeou-o-whatsapp-de-civis-sem-clicar.html>. Acesso em 07 fev. 2025.

UNIÃO EUROPEIA. Tribunal de Justiça (Grande Seção). *Acórdão de 8 de abril de 2014, Processos apensos C-293/12 e C-594/12*. Disponível em: <https://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=654354>. Acesso em: 9 fev. 2025.

UNIÃO EUROPEIA. Tribunal de Justiça (Grande Seção). *Acórdão de 6 de outubro de 2020, Processos apensos C511/18, C512/18 e C520/18*. Disponível em: <https://curia.europa.eu/juris/document/document.jsf?jsessionid=EBF20EE5EAFBB229F2CFDFB00F9E9B2A?text=&docid=232084&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=632727>. Acesso em: 9 fev. 2025, §159.

VAZ, Denise Provasi. *Provas digitais no processo penal: formulação do conceito, definição das características e sistematização do procedimento probatório*. Tese (Doutorado em 2012) – Faculdade de Direito da Universidade de São Paulo, São Paulo, 2012.

WARREN, Samuel; BRANDEIS, Louis. The right to privacy. *Harvard Law Review*, v. 4, n. 5, pp. 193-220, 1890.

WEISER, Mark. The Computer for the 21st Century. *Scientific American*, 265, September 1991.

ZANIOLO, Pedro Augusto. *Crimes modernos: o impacto da tecnologia no Direito*. 4. ed. Salvador: Editora JusPodivm, 2021.

ZUBOFF, Shoshana. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs, 2019.

INCIDENTES DE SEGURANÇA COM DADOS PESSOAIS EM SERVIÇOS DE ARMAZENAMENTO EM NUVEM: PRESERVAÇÃO DE EVIDÊNCIAS DIGITAIS E DEVERES DE COMUNICAÇÃO

Jéssica Fernandes Rocha

Mestre em Direito pela Universidade Federal de Minas Gerais (UFMG). Advogada em Privacidade, Proteção de Dados e Inteligência Artificial. Certified Data Protection Officer in Brazil (CDPO/BR) pela International Association of Privacy Professionals (IAPP). Pesquisadora do Grupo de Estudos em Direito e Tecnologia da Universidade Federal de Minas Gerais (DTEC-UFMG). Membro efetivo da Comissão de Proteção de Dados da OAB/MG. E-mail: jessica.jfr@hotmail.com

DOI: <https://doi.org/10.59224/dti7.ch3>

Resumo: Em meio ao aumento do uso corporativo de armazenamento em nuvem e ataques cibernéticos, este artigo analisa: i) a preservação de evidências digitais sob o Marco Civil da Internet ("MCI") e ii) os deveres de comunicação de incidentes à Autoridade Nacional de Proteção de Dados ("ANPD"), titulares e agentes de tratamento, conforme a Lei Geral de Proteção de Dados Pessoais ("LGPD"). Destaca-se o papel da cadeia de custódia na integridade e admissibilidade das provas digitais, com base na ISO/IEC 27037:2013, para elevar a confiabilidade das investigações e comunicações.

Palavras-chave: Incidente de Segurança, Armazenamento em Nuvem; Investigação Cibernética.

Abstract: Amid the increasing corporate use of cloud storage and cyberattacks, this article examines: i) the preservation of digital evidence under the Civil Internet Framework ("MCI") and ii) the duties to communicate incidents to the National Data Protection Authority ("ANPD"), data subjects, and data controllers, as per the General Data Protection Law ("LGPD"). It highlights the role of the chain of custody in the integrity and admissibility of digital evidence, based on ISO/IEC 27037:2013, to enhance the reliability of investigations and communications.

Keywords: Security Incident; Cloud Storage; Cyber Investigation.

SUMÁRIO: Introdução. 1. Gestão de incidentes de segurança da informação com dados pessoais; 1.1. Conceitos Elementares; 1.2. Desafios na preservação de evidências digitais; 1.3. Pontos de atenção na interpretação de evidências digitais; 1.4. Pontos de

atenção na preservação de evidências digitais; 2. Cadeia de custódia em provas digitais; 2.1. O papel da cadeia de custódia na investigação cibernética; 2.2. Um framework baseado na ISO/IEC 27037:2013; 3. Deveres de comunicação em incidentes de segurança com dados pessoais; 3.1. Categorização e comunicação entre agentes de tratamento; 3.2. Comunicação à Autoridade Nacional de Proteção de Dados; Conclusão; Referências.

INTRODUÇÃO

Um levantamento da Check Point Research reportou um aumento anual de 48% em ataques cibernéticos na nuvem para o ano de 2022, como consequência do movimento emergente das operações empresariais nestes ambientes, em um contexto de intensificação dos processos de transformação digital.¹ Assim, em que pese a crescente contratação de *Cloud Service Providers* (“CSPs”), ciberataques em nuvem têm representado sério desafio para as instituições, pois além dos danos patrimoniais e reputacionais diretos: i) as investigações cibernéticas sobre incidentes ocorridos em nuvem possuem desafios adicionais, e ii) há possibilidade da incidência de obrigações específicas da Lei Geral de Proteção de Dados Pessoais, ou Lei brasileira 13.709/2018, a serem cumpridas com diligência.

Neste contexto, pretende-se fornecer esclarecimentos à luz do Marco Civil da Internet, ou Lei brasileira 12.965/2014, sobre aspectos essenciais na preservação de evidências e interpretação das digitais, bem como pontuar questões relevantes acerca dos deveres de comunicação conexos, no âmbito da legislação de proteção de dados pessoais. Entrelaçando ambos escopos, pretende-se demonstrar, inclusive, como tais evidências podem contribuir para as comunicações em questão, integrando elementos recém regulados como o “relatório de tratamento de incidente”², previsto no artigo 3º, inciso XIX do Regulamento de Comunicação de Incidente de Segurança,

-
1. Canaltech. Ataques contra a nuvem aumentaram 48% em 2022. Disponível em: <https://canaltech.com.br/seguranca/ataques-contr-a-nuvm-aumentaram-48-em-2022-242120/>. Acesso em: 3 mai. 2024.
 2. Art. 3º, XIX. Regulamento de Comunicação de Incidente de Segurança. Disponível em: <https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024>.

1. GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO COM DADOS PESSOAIS

A investigação cibernética é um dos principais elementos da gestão de incidentes de segurança da informação, que consiste em uma abordagem sistemática para lidar com eventos que comprometam a integridade, confidencialidade e disponibilidade das informações. Nesta dinâmica, a investigação abrange ações de registro de eventos, coleta e preservação de evidências em redes computacionais, visando alcançar, principalmente, a identificação das causas, origens e o tratamento do incidente.

Esse processo envolve a identificação do incidente, avaliação de seu impacto, investigação de suas causas, sua contenção e recuperação das informações afetadas, além da implementação de medidas para mitigar riscos de novas ocorrências.³ Geralmente este processo é conduzido por uma equipe designada de profissionais de segurança da informação que são responsáveis por identificar e responder a incidentes de segurança em toda a organização.⁴

É recomendável, também, que se oriente por um Plano de Respostas a Incidentes de Segurança com Dados Pessoais previamente estabelecido, aprovado e atualizado, além de aderir a práticas padronizadas no tratamento das evidências digitais. Como pontua Mujahid, um *“planejamento proativo de resposta a incidentes, adesão a práticas padronizadas e pesquisa contínua sobre forense em nuvem são necessários para responder efetivamente a incidentes de segurança e proteger ativos digitais críticos”*.⁵

3. IFTO - Instituto Federal de Educação, Ciência e Tecnologia do Tocantins. *Política de Gestão da Segurança da Informação (PGISI)*. Disponível em: <https://portal.iftto.edu.br/acesso-a-informacao/seguranca-da-informacao/documentos-lgpd-iftto/PGISI.pdf>. Acesso em: 03.05.2024.

4. Ibidem.

5. Tradução livre. MUJAHID, Zafer. *Cloud Forensics: Investigating Security Incidents in Cloud Environments*. Lahore: Department of Computer Science, University of Garrison Lahore, 2023.

1.1. Conceitos Elementares

Compreender a dinâmica da preservação de evidências digitais em contextos de incidentes de segurança envolvendo dados pessoais em *cloud storages* demanda uma compreensão prévia sobre alguns elementos específicos. Entre estes elementos, é possível enfatizar: a) Incidente de Segurança; b) Dado Pessoal; c) Evidência Digital; e d) o enquadramento dos *Cloud Service Providers* à luz do MCI.

A Autoridade Nacional de Proteção de Dados, no Regulamento de Comunicação de Incidente de Segurança define um “incidente de segurança” como “*qualquer evento adverso confirmado, relacionado à violação das propriedades de confidencialidade, integridade, disponibilidade e autenticidade da segurança de dados pessoais*”;⁶. O regulamento ainda esclarece cada um destes conceitos, definindo: a) “confidencialidade” como “*propriedade pela qual se assegura que o dado pessoal não esteja disponível ou não seja revelado a pessoas, empresas, sistemas, órgãos ou entidades não autorizados*”; b) “integridade” como “*propriedade pela qual se assegura que o dado pessoal não foi modificado ou destruído de maneira não autorizada ou acidental*”; c) “disponibilidade” como “*propriedade pela qual se assegura que o dado pessoal esteja acessível e utilizável, sob demanda, por uma pessoa natural ou determinado sistema, órgão ou entidade devidamente autorizados*”; e d) “autenticidade” como “*propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade*”.

O art. 5º, inciso I da LGPD define dado pessoal como “*informação relacionada a pessoa natural identificada ou identificável*”;⁷. Para os fins deste trabalho, é justamente o comprometimento desta natureza de dados que fará incidir as obrigações de comunicação decorrentes da Lei Geral de Proteção de Dados Pessoais, melhor abordadas no tópico 3 deste trabalho. O Regulamento esclarece que entende-

6. BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). *Resolução ANPD nº 15, de 24 de abril de 2024*. Art. 3º, XII. Disponível em: <https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024>. Acesso em: 2 jul. 2024.

7. Art. 5º, I. LGPD. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2020]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/114020.htm. Acesso em: 14 abr. 2021.

Incidentes de segurança com dados pessoais em serviços de armazenamento em nuvem
se como “dado pessoal afetado” aquele “cuja *confidencialidade, integridade, disponibilidade ou autenticidade tenha sido comprometida em um incidente de segurança*”.

Evidências digitais, conforme a ABNT/ISO 27037 (“ISO 27037”), podem ser definidas como “*informações ou dados, armazenados ou transmitidos em forma binária, que podem ser invocados como evidência*”⁸. Alessandro Barreto e Beatriz Brasil ensinam que a interação que o criminoso realiza com a máquina gera algo que pode ser entendido como uma “impressão digital virtual”⁹. Alguns exemplos de evidências digitais são logs de acesso, arquivos temporários, cookies e horário de inicialização de um dispositivo.

O art. 5º, inciso VII do MCI conceitua “aplicações de internet” como o “*conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet*”¹⁰. Assim, um provedor de aplicação pode ser identificado pelo fornecimento de um “*conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet, não importando se os objetivos são econômicos*”¹¹. À luz do MCI os *Cloud Service Providers* podem ser enquadrados como provedores de aplicações de internet, atraindo as respectivas obrigações quanto ao armazenamento de registro de acesso às aplicações fornecidas, conforme o art. 15 do mesmo diploma. Isso porque os CSPs oferecem funcionalidades como armazenamento, processamento de dados, e outras atividades acessíveis por meio da rede mundial de computadores.

8. De acordo com o item 3.5. da norma ABNT NBR ISO/IEC 27037.

9. BARRETO, Alessandro Gonçalves; BRASIL, Beatriz Silveira. *Manual de investigação cibernética: à luz do marco civil da internet*. Imprensa: Rio de Janeiro, Brasport, 2016. p. 54.

10. BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Diário Oficial [da República Federativa do Brasil], Poder Legislativo, Brasília, DF, 23 abr. 2014. Disponível em: <http://www.planalto.gov.br/CCI-VIL_03/_Ato2011-2014/2014/Lei/L12965.htm>. Acesso em: 29 maio 2014.

11. CERÓY, Frederico Meinberg. *Os conceitos de provedores do Marco Civil da Internet*. Set. 2014. JusNavigandi. Disponível em: <https://jus.com.br/artigos/31938/os-conceitos-de-provedores-no-marco-civil-da-internet#google_vignette>. Acesso em: 9 mar. 2016.

1.2. Desafios na preservação de evidências digitais

A preservação de evidências digitais é um ponto crucial e que deve ser cuidadosamente observado em razão da volatilidade dos dados em ambiente digital, podendo ser rapidamente manipulados, alterados ou deletados. Alessandro Barreto e Beatriz Brasil e ensinam que a evidência cibernética “*caracteriza-se por ser volátil, anônima (em princípio), alterável e/ou modificável, bem como pode ser eliminada a qualquer instante.*”¹²

Neste contexto, os cibercrimes “*se fundamentam principalmente nas dificuldades que a força investigativa enfrenta para recolher provas que sejam suficientes para instauração do processo penal*”¹³. Vale ressaltar, ainda, que apesar de não consistir em um diploma legal focado na investigação de cibercrimes, o Marco Civil da Internet contribuiu expressivamente para consolidações no tema, estabelecendo requisitos, prazos, e limitações aos procedimentos da investigação cibernética.¹⁴

Nota-se que para além dos desafios na preservação de evidências digitais, por si só, investigações cibernéticas em ambientes de armazenamento em nuvem possuem particularidades que as tornam ainda mais complexas. O item 5.4.2. da norma ISO 27037, melhor discutida no tópico 2.2 deste trabalho, ressalta que “*nem todos os tipos de mídia de armazenamento digital podem ser facilmente identificados e localizados, por exemplo, computação em nuvem*”.¹⁵ Neste sentido, Heiser reforça:

“*Serviços de Cloud são especialmente difíceis de investigar, porque os logs e dados de vários clientes podem estar localizados conjuntamente e também estar distribuídos com uma constante mudança no conjunto de máquinas e data centers*”. (grifou-se)¹⁶

12. BARRETO, Alessandro Gonçalves; BRASIL, Beatriz Silveira. *Manual de investigação cibernética: à luz do marco civil da internet*. Imprensa: Rio de Janeiro, Brasport, 2016. p. 53.

13. DA SILVA, Rosane Leal; DALLA FAVERA, Rafaela Bolson; DE QUADROS OLMOS, Olívia Martins. *A responsabilidade civil dos principais cloud computing providers em razão da perda de arquivos*. Revista da Faculdade de Direito UFPR, 2018, 63.2: 89-113.

14. BARROSO, Carolina Rodrigues de Carvalho. *Meios de investigação e produção de provas nos crimes cibernéticos*. Universidade Federal Fluminense, Niterói, 2019. p. 40

15. Item 5.4.2. da versão brasileira da norma, ABNT NBR ISO/IEC 27037.

16. HEISER, Jay. *What You Need to Know About Cloud Computing Security and Compliance*. Disponível em: Acesso em 02 jul. 2024.

Sobre a ponderação entre benefícios e riscos de segurança da informação associados ao *cloud storage*, Barreto e Brasil pontuam:

“É certo que o armazenamento em nuvem diminui custos para as empresas, havendo o aumento da procura desse serviço e, via de consequência, potencializando-se o risco de violação de dados. Além do mais, há, em tese, a perda do controle dos dados pelo seu proprietário, uma vez que a guarda desse conteúdo ocorre em locais diversos”. (grifou-se)¹⁷

Moses Ashawa *et al.* alertam sobre os desafios notados nas investigações forenses aplicadas sobre ambientes em nuvem:

“Dada a crescente prevalência do trabalho remoto e a necessidade de as empresas serem adaptáveis e reagirem rapidamente às mudanças nas circunstâncias do mercado, a infraestrutura em nuvem tornou-se um ativo crucial para organizações de várias escalas. Embora a nuvem ofereça benefícios como escalabilidade, flexibilidade e colaboração aprimorada, ela apresenta dificuldades nas investigações forenses digitais em relação à proteção de dados, propriedade e limites jurisdicionais”.(grifou-se)¹⁸

Moses Ashawa *et al.* também destacam a importância de que a comunidade científica trabalhe em conjunto para estabelecer uma abordagem padronizada para as investigações forenses digitais na nuvem, assegurando que as provas sejam recolhidas e analisadas de forma sistemática e transparente. Esta evolução possui o potencial de contribuir incisivamente para a confiabilidade e a precisão das investigações, aspectos que representam desafio para investigadores e analistas forenses.¹⁹

A perícia em nuvem analisa logs, controles de acesso e atividades do usuário para

17. BARRETO, Alessandro Gonçalves; BRASIL, Beatriz Silveira. *Manual de investigação cibernética: à luz do marco civil da internet*. Imprensa: Rio de Janeiro, Brasport, 2016. p. 160.

18. Tradução livre. ASHAWA, Moses;MANSOUR, Ali;RILEY, Jackie;OSAMOR, Jude; OWOH, Nsikak.Digital Forensics Challenges in Cyberspace: Overcoming Legitimacy and Privacy Issues Through Modularisation. Cloud Computing and Data Science, 2023, 140-156. 10.37256/ccds.5120233845.

19. ASHAWA, Moses;MANSOUR, Ali;RILEY, Jackie;OSAMOR, Jude; OWOH, Nsikak. Digital Forensics Challenges in Cyberspace: Overcoming Legitimacy and Privacy Issues Through Modularisation. Cloud Computing and Data Science, 2023, 140-156. 10.37256/ccds.5120233845.

identificar vulnerabilidades na infraestrutura de nuvem que levam a violações de dados.²⁰ Este processo auxilia as organizações a incrementarem os níveis de segurança, além de recuperar dados comprometidos ou excluídos em ambientes complexos.²¹ Malik destaca desafios e pontos de atenção nestes contextos, dentre eles a importância da colaboração dos provedores de serviços em nuvem:

“(...) especialistas enfrentam desafios tecnológicos e legais na governança de dados transfronteiriços, necessitando de colaboração com provedores de serviços em nuvem. A perícia em nuvem é crucial para investigar incidentes, preservar evidências, mitigar consequências, proteger dados confidenciais e manter a confiança no ecossistema digital”²² (grifou-se)

Mujahid pontua que *“as implicações legais e de privacidade da análise forense em nuvem são significativas, especialmente no que diz respeito a transferências transfronteiriças de dados e desafios jurisdicionais”²³*. Easwaramoorthy *et al.* também consideram que a ausência de um bom relacionamento com outros países pode dificultar o processo de coleta das provas e causar atrasos no processo de investigação forense.²⁴

No que tange à troca de informações entre países sobre crimes cibernéticos, vale

-
20. RAGHAVENDRA, S. *et al.* *Critical retrospection of security implication in cloud computing and its forensic applications*. Security and Communication Networks, v. 2022, artigo 1791491, 2022. Disponível em: <https://doi.org/10.1155/2022/1791491>. Acesso em: 2 jul. 2024.
 21. SURANGE, G.; KHATRI, P. *IoT forensics: A review on current trends, approaches and foreseen challenges*. In: Proceedings of the 2021 8th International Conference on Computing for Sustainable Global Development (INDIACom), 17-19 March 2021, New Delhi, India. Piscataway: IEEE, 2021. p. 909-913.
 22. MALIK, Annas Wasim *et al.* *Cloud digital forensics: beyond tools, techniques, and challenges*. Sensors, Basel, v. 24, n. 2, p. 433, 2024. Disponível em: <https://doi.org/10.3390/s24020433>. Acesso em: 2 jul. 2024.
 23. MUJAHID, Zafer. *Cloud Forensics: Investigating Security Incidents in Cloud Environments*. Lahore: Department of Computer Science, University of Garrison Lahore, 2023. p. 6.
 24. EASWARAMOORTHY, S.; THAMBURASA, S.; SAMY, G.; BHUSHAN, S. B.; ARAVIND, K. *Digital forensic evidence collection of cloud storage data for investigation*. In: INTERNATIONAL CONFERENCE ON RECENT TRENDS IN INFORMATION TECHNOLOGY (ICRTIT), 2016, Chennai. Anais [...]. Chennai: IEEE, 2016. p. 1-6. doi: 10.1109/ICRTIT.2016.7569516. p. 3.

Incidentes de segurança com dados pessoais em serviços de armazenamento em nuvem ressaltar que a Convenção de Budapeste sobre o Cibercrime²⁵ contribui ao estabelecer diretrizes internacionais para a cooperação, facilitando a obtenção de evidências digitais transnacionais.²⁶ O diploma foi incorporado ao ordenamento jurídico brasileiro pelo Decreto 11.491 de 12 de abril de 2023 e facilita a colaboração entre países na investigação e combate aos crimes cibernéticos.²⁷ Sua principal contribuição para o contexto em tela é estabelecer procedimentos comuns para o acesso e preservação de dados eletrônicos, reduzindo conflitos de jurisdição.

Por serem notórios os desafios no tratamento de evidências digitais, o artigo 4º da Lei nº 12.735/2012 estabelece que “os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado”. Apesar de o dispositivo ainda não ter sido regulamentado, diversos estados brasileiros - como Bahia, Espírito Santo, Minas Gerais, Pará, Paraná, Piauí, Rio de Janeiro, Rio Grande do Sul, São Paulo e Sergipe - já contam com delegacias ou setores especializados.²⁸

1.3. Pontos de atenção na interpretação de evidências digitais

Entre as possíveis evidências digitais, os logs possuem um papel central na condução das investigações cibernéticas. Um artigo publicado na página da American Bar Association (ABA) ilustra a importância dos logs na interpretação de questões relativas ao fato investigado, especialmente para limitar o escopo de uma violação. Ilustra-se:

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

26. PEGORARO DE ARAUJO, C. V. *Os Aspectos Gerais Dos Tratados Internacionais e a Convenção de Budapeste Sobre Crimes Cibernéticos*. Revista Da Faculdade De Direito Da Universidade Federal De Uberlândia, 50(1), 2022, 145–165. <https://doi.org/10.14393/RFADIR-50.1.2022.65259.145-165>

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

28. BARRETO, Alessandro Gonçalves; BRASIL, Beatriz Silveira. *Manual de investigação cibernética: à luz do marco civil da internet*. Imprensa: Rio de Janeiro, Brasport, 2016. p. 165.

*“A revisão de logs é frequentemente o ponto de partida para investigadores forenses, pois ajuda a identificar o método de acesso à rede, quais contas de usuário foram potencialmente comprometidas, evidências de uma atividade de comando e controle e qualquer evidência de exfiltração de dados, como grandes transferências de dados para endereços IP externos suspeitos. Os logs sempre correm o risco de serem substituídos e devem ser imediatamente preservados. Dados vitais de logs incluem logs de firewall, logs de VPN, logs de e-mail, logs de detecção de intrusão e logs de detecção de endpoint”.*²⁹ (grifou-se)

Easwaramoorthy et al., no paper “*Digital Forensic Evidence Collection of Cloud Storage Data for Investigation*”, sintetizaram potenciais contribuições das evidências coletadas na compreensão de aspectos relacionados ao ocorrido:

*“Após realizar este exame forense e análise dos provedores de serviço One Drive e Amazon Cloud Drive, os investigadores descobriram que, durante as etapas iniciais de uma análise, será necessário identificar as informações do provedor de serviços e seus detalhes correspondentes da conta do usuário. Essas informações da conta do usuário ajudarão o investigador a prever a localização dos dados do usuário e tomar as medidas adequadas para coletar, analisar e proteger essas evidências de maneira oportuna. Foi constatado que um investigador pode prever detalhes de uso da conta de armazenamento em nuvem realizando várias atividades, como comparação de hash, análise de Registro, análise de RAM, buscas por palavras-chave e análise de tráfego de pacotes de rede”.*³⁰ (grifou-se)

Além disso, compreender alguns aspectos técnicos inerentes às evidências digitais, tais como aqueles referentes aos endereços de IP e portas lógicas pode contribuir consideravelmente para as investigações de incidentes de segurança, especialmente se tratando de ataques cibernéticos. Primeiramente, cumpre esclarecer que o endereço IP (*Internet Protocol*) colabora na identificação do

29. Tradução livre. ASSOCIAÇÃO AMERICANA DE ADVOGADOS. *Evidence Preservation*. Disponível em: https://www.americanbar.org/groups/tort_trial_insurance_practice/committees/cyber-data-privacy/evidence-preservation/. Acesso em: 3 jul. 2024.

30. EASWARAMOORTHY, S.; THAMBURASA, S.; SAMY, G.; BHUSHAN, S. B.; ARAVIND, K. *Digital forensic evidence collection of cloud storage data for investigation*. In: INTERNATIONAL CONFERENCE ON RECENT TRENDS IN INFORMATION TECHNOLOGY (ICRTIT), 2016, Chennai. Anais [...]. Chennai: IEEE, 2016. p. 1-6. doi: 10.1109/ICRTIT.2016.7569516. p. 6-7.

Incidentes de segurança com dados pessoais em serviços de armazenamento em nuvem

dispositivo na rede, como um computador ou um servidor, afunilando o rastreamento da origem e o destino da comunicação. O IP pode ser utilizado para localizar geograficamente determinado dispositivo e associá-lo a um usuário ou organização, contribuindo para identificar os atacantes ou os alvos em um ataque cibernético.

As portas lógicas, por sua vez, “*designam uma sequência numérica adicional utilizada em conjunto com número IP para identificar a localização de dispositivos conectados à internet*”³¹. Desta forma, podem contribuir incisivamente para a identificação de um terminal específico. Em apertada síntese, isso ocorre porque, em muitas redes, especialmente em redes domésticas ou empresariais, todos os dispositivos da rede interna apresentam o mesmo endereço IP, mas são diferenciados internamente por portas lógicas. Sobre este ponto, esclarece o Instituto de Referência em Internet e Sociedade (IRIS):

“Por meio do gerenciamento das portas lógicas, poderá compartilhar um IP global entre vários dispositivos conectados, sabendo a origem e destino de cada pacote endereçado ao roteador. Mesmo que todos os pacotes sejam destinados a um mesmo IP, serão diferenciados pelo roteador do provedor, por meio da tabela de vinculação e das portas lógicas a eles anexadas”.³² (grifou-se)

Em síntese, o endereço IP e as portas lógicas permitem uma análise detalhada do tráfego da rede, colaborando para a reconstrução dos eventos que levaram ao ataque, identificando as vulnerabilidades exploradas, e estabelecendo uma cadeia de evidências para investigação do incidente. Esta cadeia e sua devida interpretação, possuem um importante papel nas comunicações sobre o incidente de segurança perante à ANPD, como será demonstrado no tópico 3.2 deste artigo, considerando casos em que sejam comprometidos dados pessoais.

31. INSTITUTO DE REFERÊNCIA EM INTERNET E SOCIEDADE (Brasil) (Org.). *Portas lógicas e registros de acesso*: das possibilidades técnicas aos entendimentos dos tribunais brasileiros. Belo Horizonte: Iris, 2017. Disponível em: https://irisbh.com.br/wp-content/uploads/2017/11/Portas-L3gicas-e-Registros-de-Acesso_PT.pdf. Acesso em: 02/07/2024.

32. Ibidem.

1.4. Pontos de atenção na preservação de evidências digitais

Os logs de acesso a aplicações na internet são mencionados pelo MCI como “conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP”³³. Chung et al. ensinam que “o arquivo de log desempenha um papel substancial na análise forense digital para revelar ações ocultas do invasor registrando suas etapas sequenciais”.³⁴

Barreto e Brasil ensinam que incumbe ao responsável pela investigação cibernética a identificação, coleta e a análise da evidência digital de modo adequado. Para isso, é necessário que a integridade e a autenticidade da informação sejam demonstradas por meio da cadeia de evidências, comprovando que i) “a informação obtida é a representação dos dados originais extraídos da aplicação de internet”³⁵; e ii) “os passos para a preservação da evidência foram seguidos e o conteúdo não sofreu alteração.”³⁶

O Marco Civil possibilita que a autoridade policial e o Ministério Público realizem requerimento cautelar para preservação dos registros de conexão bem como os de acesso a aplicações de internet. Nos termos do art. 15 do MCI, tais registros devem ser mantidos pelo provedor por 06 meses. Este prazo pode ser estendido por mediante determinação judicial via requerimento da autoridade policial, administrativa ou do Ministério Público, conforme o art. 15, § 2º do MCI. Neste caso, aplica-se o prazo de 60 dias para ingressar judicialmente com pedido de autorização de acesso aos registros, nos termos do art. 13, § 3º, sob pena de perda de eficácia ou indeferimento, como dispõe o § 4º do mesmo artigo. Ressalta-se que o provedor de aplicação de internet deverá manter sigilo quanto ao requerimento, em alinhamento

33. Art. 5º, inciso VIII. BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Diário Oficial [da República Federativa do Brasil], Poder Legislativo, Brasília, DF, 23 abr. 2014. Disponível em: <http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2014/Lei/L12965.htm>. Acesso em: 29 maio 2014.

34. Tradução livre. Chung, J. Park, S. Lee, and C. Kang. *Digital forensic investigation of cloud storage services*. Digital Invest. 9, 2, 2012, 81–95.

35. BARRETO, Alessandro Gonçalves; BRASIL, Beatriz Silveira. Manual de investigação cibernética: à luz do marco civil da internet. Imprensa: Rio de Janeiro, Brasport, 2016. p. 54.

36. Ibidem.

Incidentes de segurança com dados pessoais em serviços de armazenamento em nuvem
ao art. 13, § 4º.

Ainda no âmbito da análise de dispositivos específicos do MCI, nota-se que os arts. 10 e 7º, inciso III, são especialmente relevantes para o contexto em análise. No âmbito de um incidente de segurança no *cloud storage* de uma organização, surge a necessidade de obter logs de acesso ao sistema para investigar o incidente. O art. 7º, inciso III, dispõe sobre a “*inviolabilidade e sigilo de suas comunicações privadas armazenadas*”, garantindo que qualquer acesso a essas informações seja amparado por uma mediante ordem judicial.

O art. 10 do MCI, por sua vez, determina que os registros de conexão e de acesso a aplicações de internet devem ser armazenados de maneira a garantir a privacidade dos usuários e o sigilo das comunicações. O § 1º do dispositivo prevê que “*o provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial*”. Assim, para obter logs de acesso e outras evidências digitais de um provedor de armazenamento em nuvem, a organização deve solicitar uma ordem judicial.

Essa exigência visa proteger a privacidade dos dados dos usuários e assegurar que a disponibilização dessas informações seja justificada e legitimada judicialmente. Ou seja, na dinâmica sistemática destas previsões fica estabelecida a obrigatoriedade dos provedores de preservar e fornecer registros de acesso e atividades sob demanda judicial, enquanto resguarda-se a privacidade e sigilo das comunicações privadas dos usuários. Isso cria um equilíbrio entre a necessidade de investigar incidentes de segurança e a proteção dos direitos dos usuários.

Neste cenário, a organização que identifica um incidente de segurança e necessidade de evidências digitais a serem fornecidas pelo CSP do seu serviço de armazenamento deve apresentar um pedido ao judiciário. Este requerimento deve fundamentar a necessidade dos registros e logs de acesso para a investigação do incidente de segurança, sendo crucial que, em contextos adequados, haja a cooperação destes provedores, conforme pontua Mujahid:

“*Preservar a integridade das evidências digitais na nuvem é crucial para garantir sua admissibilidade em processos legais. A cooperação dos provedores de serviços em*

*nuvem é essencial para acessar e preservar as evidências, destacando a importância da colaboração entre investigadores e provedores de nuvem”.*³⁷

Caso o pedido seja deferido, uma ordem judicial é emitida ao provedor para que disponibilize os registros em questão. Assim, ao receber a ordem judicial, o *Cloud Provider* deve fornecer os registros e logs solicitados, mantendo a integridade e autenticidade das evidências. Este processo assegura que a coleta de evidências digitais em casos de incidentes de segurança no armazenamento em nuvem seja feita em conformidade com as leis brasileiras, em alinhamento aos direitos dos titulares e garantindo a validade das evidências coletadas para possíveis processos judiciais ou administrativos.

Ainda cumpre pontuar que a obrigação de que os provedores de aplicações mantenham os registros de acesso às aplicações em ambiente controlado contribui para que os *Cloud Service Providers* a identifiquem e corrijam as falhas em seus sistemas. Isso evita futuras perdas ou extravios de arquivos pertencentes aos seus consumidores.³⁸ A dinâmica é benéfica porque, via de regra, o foco destes provedores consiste em garantir a disponibilidade do serviço, e não em armazenar evidências.³⁹

Outro ponto de destaque seria que, apesar de as portas lógicas não constarem expressamente previstas no artigo 15 do MCI dentre as informações a serem armazenadas pelos provedores, dada sua importância na identificação de terminais, é possível embasar sua exigibilidade diante do provedor. Isso se deve à interpretação centrada no propósito da norma, qual seja, reunir informações que efetivamente possibilitem a identificação do dispositivo utilizado.

No julgamento do Recurso Especial (REsp) nº 1.784.156/SP no Superior Tribunal de Justiça (STJ), restou consolidado que a individualização da navegação na internet passa a depender da porta lógica pela necessidade de compartilhamento de endereços

37. Tradução livre. MUJAHID, Zafer. *Cloud Forensics: Investigating Security Incidents in Cloud Environments*. Lahore: Department of Computer Science, University of Garrison Lahore, 2023.

38. DA SILVA, Rosane Leal; DALLA FAVERA, Rafaela Bolson; DE QUADROS OLMOS, Olívia Martins. *A responsabilidade civil dos principais cloud computing providers em razão da perda de arquivos*. Revista da Faculdade de Direito UFPR, 2018, 63.2: p. 107.

39. Hamilton José Sales Fonte II. *Dizang: uma solução para coleta de evidências forenses para ataques de injeção na nuvem*. P. 31. Dissertação de Mestrado. USP. Disponível em: <https://teses.usp.br/teses/disponiveis/3/3141/tde-07022020-111602/pt-br.php>. Acesso em: 03.05.2024.

Incidentes de segurança com dados pessoais em serviços de armazenamento em nuvem de IP. Conforme destacado a seguir, interpretou-se no sentido de que “a revelação das portas lógicas de origem consubstancia simples desdobramento lógico do pedido de identificação do usuário por IP”. Ilustra-se:

RECURSO ESPECIAL. CIVIL E PROCESSUAL CIVIL. AÇÃO DE OBRIGAÇÃO DE FAZER. PROVEDOR DE APLICAÇÕES. IDENTIFICAÇÃO DO DISPOSITIVO UTILIZADO PARA ACESSO À APLICAÇÃO. INDICAÇÃO DO ENDEREÇO IP E PORTA LÓGICA DE ORIGEM. INTERPRETAÇÃO TELEOLÓGICA DOS ARTS. 5º, VII, E 15 DA LEI N. 12.965/2014. RECURSO ESPECIAL PROVIDO.

(...) 2. A previsão legal de guarda e fornecimento dos dados de acesso de conexão e aplicações foi distribuída pela Lei n. 12.965/2014 entre os provedores de conexão e os provedores de aplicações, em observância aos direitos à intimidade e à privacidade.

3. Cabe aos provedores de aplicações a manutenção dos registros dos dados de acesso à aplicação, entre os quais se inclui o endereço IP, nos termos dos arts. 15 combinado com o art. 5º, VIII, da Lei n. 12.965/2014, os quais poderão vir a ser fornecidos por meio de ordem judicial.

4. A obrigatoriedade de fornecimento dos dados de acesso decorre da necessidade de balanceamento entre o direito à privacidade e o direito de terceiros, cujas esferas jurídicas tenham sido aviltadas, à identificação do autor da conduta ilícita.

5. Os endereços de IP são os dados essenciais para identificação do dispositivo utilizado para acesso à internet e às aplicações.

6. A versão 4 dos IPs (IPv4), em razão da expansão e do crescimento da internet, esgotou sua capacidade de utilização individualizada e se encontra em fase de transição para a versão 6 (IPv6), fase esta em que foi admitido o compartilhamento dos endereços IPv4 como solução temporária.

7. Nessa fase de compartilhamento do IP, a individualização da navegação na internet passa a ser intrinsecamente dependente da porta lógica de origem, até a migração para o IPv6.

8. A revelação das portas lógicas de origem consubstancia simples desdobramento lógico do pedido de identificação do usuário por IP.

9. Recurso especial provido⁴⁰.

Assim, o julgado do STJ chancela o entendimento de que as portas lógicas poderiam ser exigidas dos provedores de aplicação internet dado seu papel na identificação de terminais específicos. Isso porque a realidade técnica atual revela um contexto de compartilhamento de endereços de IP por diversos dispositivos conectados a redes domésticas e empresariais. Assim, o dever dos provedores em manter os registros de acesso às suas aplicações, enquadrados como “*o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP*”⁴¹, desdobra-se no fornecimento, também, das respectivas portas lógicas.

2. CADEIA DE CUSTÓDIA EM PROVAS DIGITAIS

No campo das investigações cibernéticas, a cadeia de custódia é um elemento de suma importância na garantia da integridade e admissibilidade e legitimidade destas evidências em processos administrativos e judiciais conexos. Os procedimentos de documentação e manuseio que compõem a cadeia de custódia são essenciais para manter a credibilidade das evidências desde o ponto de coleta até sua apresentação em contextos determinantes como os procedimentos administrativos instaurados sob a competência da ANPD.

Assim, é recomendável observar um *framework* abrangente e consolidado na cadeia de custódia, como a norma ISO/IEC 27037:2013. Esta normativa fornece diretrizes detalhadas para a identificação, coleta, aquisição e preservação de evidências digitais, oferecendo uma metodologia robusta para investigações digitais. Assim, nos tópicos 2.1 e 2.2 a seguir busca-se destacar a interseção entre os princípios legais e os padrões técnicos na otimização dos processos que sustentam a eficácia da investigação forense. Malik *et al.* ensinam que a necessidade de uma abordagem abrangente “*está alinhada à natureza dinâmica da investigação forense digital baseada na nuvem, garantindo que os especialistas possam navegar eficazmente em*

40. BRASIL. Superior Tribunal de Justiça. *Recurso Especial n. 1.784.156/SP*. Relator Ministro Marco Aurélio Bellizze, Terceira Turma, julgado em 5 nov. 2019, Diário da Justiça Eletrônico, 21 nov. 2019.

41. Nos termos do art. 5º VIII, do MCI.

Incidentes de segurança com dados pessoais em serviços de armazenamento em nuvem
*diversos desafios, ao mesmo tempo que respeitam os padrões éticos e legais*⁴².

2.1. O papel da cadeia de custódia na investigação cibernética

Num contexto de preservação de evidências digitais é muito importante ter atenção à cadeia de custódia, visto que no ordenamento jurídico brasileiro, a admissibilidade destas evidências não é incondicionada. Há diversos dispositivos jurídicos que estabelecem questões a serem observadas, especialmente no âmbito de processos penais. Em uma aplicação prática isso significa que diversos procedimentos devem ser rigorosamente observados para garantir a integridade, autenticidade e admissibilidade das provas digitais ao longo de todo o processo investigativo, de modo que possam ser aproveitadas em procedimentos administrativos e judiciais cabíveis.

A Constituição Federal de 1988, no artigo 5º, inciso LVI, estabelece que *"são inadmissíveis, no processo, as provas obtidas por meios ilícitos"*. Esse artigo destaca a importância da legalidade na obtenção e preservação de provas, o que engloba as digitais, reforçando a necessidade de seguir procedimentos adequados para garantir a legitimidade e admissibilidade das evidências. O Pacote Anticrime (Lei nº 13.964/2019), em seu artigo 158-A, define claramente o conceito de cadeia de custódia como *"o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte"*.

Assim, é recomendável seguir metodologias padronizadas aplicáveis ao contexto, tal como norma ABNT NBR ISO/IEC 27037:2013. Ressalta-se que as normas ISO/IEC são elaboradas pela Organização Internacional de Padronização (ISO) em trabalhos conjuntos com a Comissão Eletrotécnica Internacional (IEC) visando otimizar a qualidade de produtos e serviços. No Brasil, estas normas são acrescidas da sigla NBR (Norma Brasileira), devido à revisão e gerenciamento que se submetem

42. Tradução livre. MALIK, Annas Wasim *et al.* *Cloud digital forensics: beyond tools, techniques, and challenges*. Sensors, Basel, v. 24, n. 2, p. 433, 2024. Disponível em: <https://doi.org/10.3390/s24020433>. Acesso em: 2 jul. 2024.

por parte da Associação Brasileira de Normas Técnicas (ABNT).⁴³

2.2. Um *framework* baseado na ISO/IEC 27037:2013

Um *framework* que apresenta grande utilidade no texto em análise é a ABNT NBR ISO/IEC 27037:2013 - “*Diretrizes para identificação, coleta, aquisição e preservação de evidência digital*”. Em vigor no Brasil desde 2014, a norma é considerada referência internacional para o tratamento de evidências forenses digitais em todas as etapas do processo de investigação, fornecendo diretrizes para atividades específicas no manuseio destas informações. A norma integra a família ISO 27000 - Gestão da Segurança da Informação, sendo a mais relevante no âmbito da perícia forense digital.

Sua metodologia agrega procedimentos que abrangem a identificação, coleta, aquisição e preservação de evidências com potencial valor probatório. Ela fornece orientação a indivíduos com relação a situações comuns encontradas ao longo do tratamento de evidências digitais e auxilia as organizações a padronizarem este tratamento, o que contribuirá para sua relevância, admissibilidade, força probatória e em eventuais processos administrativos e judiciais.

A ISO 27037 se aplica a uma ampla gama de dispositivos digitais e, dentre eles, se aplica aos meios de armazenamento digital em computadores, que por sua vez engloba a modalidade “*Cloud Storage*”.⁴⁴ Ela concentra-se em dados que encontram-se em formato digital e possuem potencial valor probatório em determinado processo. Assim, os indivíduos que lidam com evidências digitais “*devem ser capazes de identificar e gerenciar os riscos que podem surgir ao trabalhar com esse tipo de evidência, a fim de evitar sua degradação e torná-la inútil*”.⁴⁵

43. Conteúdo Jurídico. *Cadeia de custódia da prova na investigação criminal em ambiente digital*. Disponível em: <https://conteudojuridico.com.br/consulta/Artigos/58599/cadeia-de-custdia-da-prova-na-investigao-criminal-em-ambiente-digital>. Acesso em: 2 jul. 2024.

44. BRASIL, Eandro Cleiton Araújo. *Identificação e análise das ferramentas de computação forense aplicadas em investigações no Brasil*. 2023. 79 f. Trabalho de Conclusão de Curso (Graduação em Sistema de Informação)- Universidade Federal do Ceará, Campus de Quixadá, Quixadá, 2023. p. 38.

45. Tradução livre. VEBER, Jaromír; SMUTNY, Zdenek. Standard ISO 27037:2012 and Collection of

Apesar de não se tratar de norma cogente devido ao fato de não haver um reconhecimento positivado em lei, é a única norma elaborada por um organismo competente e reconhecido no Brasil, qual seja a ABNT (Associação Brasileira de Normas Técnicas), órgão responsável pela normalização técnica no Brasil.⁴⁶ Além disso, a norma em sua versão internacional (ISO), descreve procedimentos adotados em alinhamento aos ordenamentos de muitos países. Assim, a doutrina defende pela aplicação da Norma ABNT NBR ISO/IEC 27037:2013, na padronização do tratamento de evidências digitais.⁴⁷

Em seu item 5.2, “*Princípios da evidência digital*”, a norma dispõe que toda evidência digital válida deve apresentar 03 características fundamentais: a) relevância; b) confiabilidade e c) suficiência. A “relevância” estaria relacionada a sua aptidão em provar ou refutar um elemento integrante do contexto investigado. A “confiabilidade” estaria ligada à necessidade de que todos os processos usados no tratamento de possíveis evidências digitais sejam auditáveis e repetíveis, atestando a fidelidade de um dado em relação ao original. Já a “suficiência” seria concebida na medida em que a evidência digital baste para permitir que elementos questionados sejam adequadamente investigados ou examinados.⁴⁸

A “auditabilidade”⁴⁹ e a “repetibilidade”⁵⁰, vinculados ao atributo da “confiabilidade”, também são detalhadas pela norma. A “auditabilidade” torna possível que um avaliador independente ou outras partes interessadas e autorizadas avaliem as atividades realizadas pelo DEFR (“*Digital Evidence First Responder*”)⁵¹ ou

Digital Evidence: Experience in the Czech Republic. European Conference on Information Warfare and Security, ECCWS. 2015. 294-299.

46. NETO, M. F.; SANTOS, J. E. L. d. *Apontamentos sobre a cadeia de custódia da prova digital no Brasil*. Em Tempo, v. 20, 2020.

47. MACHADO, Leonardo Marcondes. *Aplicação da cadeia de custódia da prova digital*. Revista Consultor Jurídico, 2020. 6p. Disponível em: <https://www.conjur.com.br/2020-mar-31/academiapolicia-aplicacao-cadeia-custodia-prova-digital>. Acesso em: 30 jun. 2024.

48. NETO, M. F.; SANTOS, J. E. L. d. *Apontamentos sobre a cadeia de custódia da prova digital no Brasil*. Em Tempo, v. 20, 2020.

49. Item 5.3.2 da ISO 27037.

50. Item 5.3.3 da ISO 27037.

51. De acordo com o item 3.7. da versão brasileira da norma, ABNT NBR ISO/IEC 27037, o DEFR seria o “Primeiro Interventor de Evidências Digitais”, pode ser entendido como um profissional

pelo DES (*“Digital Evidence Specialist”*)⁵² no tratamento das evidências. Já a repetibilidade pode ser entendida como a *“propriedade de um processo para obter os mesmos resultados de teste em um diferente ambiente de teste”*.⁵³ Ou seja, um DEFR deve ser capaz de realizar todos os processos descritos na documentação e alcançar os mesmos resultados, sem orientação ou interpretações avulsas.⁵⁴

O item 5.4, *“Processo de manuseio da evidência digital”*, detalha o passo-a-passo a ser observado no tratamento dessas informações. A primeira etapa na cadeia de custódia é o reconhecimento de um incidente de segurança. Vale ressaltar que ferramentas de monitoramento de segurança e logs de atividade podem apresentar grande utilidade nesta fase para detectar incidentes. Este processo envolve a identificação de anomalias ou atividades suspeitas que indicam uma potencial violação de segurança em um ambiente. Para os fins deste trabalho, esta etapa poderia consistir, por exemplo, na identificação da violação de um *cloud storage*, no qual são armazenados ativos da organização.

Após reconhecer um incidente, a norma indica ser crucial identificar todas as possíveis fontes de evidências digitais. Em um ambiente de nuvem, essas fontes podem incluir logs de servidores, registros de auditoria, snapshots de máquinas virtuais, backups, arquivos armazenados, metadados e registros de rede. É importante mapear todas essas fontes para garantir uma coleta abrangente de evidências digitais que observem os princípios e procedimentos descritos.

Assim, deve-se proceder à avaliação da relevância das informações disponíveis, pois nem todos os dados identificados serão relevantes para a investigação. Reitera-se que a relevância é uma característica fundamental das evidências digitais, nos termos do item 5.2, *“Princípios da evidência digital”*. Desta forma, uma avaliação inicial deve ser realizada a fim determinar quais dados são pertinentes para a análise

que possui as habilidades e conhecimentos necessários para identificar, coletar, adquirir e preservar evidências digitais de maneira que sua integridade e autenticidade sejam mantidas.

52. De acordo com o item 3.8. da versão brasileira da norma, ABNT NBR ISO/IEC 27037, o DES seria o “Especialista em Evidências Digitais”, enquadrado como um profissional que além de ser capaz de realizar as tarefas de um DEFR, também possui *“conhecimento especializado, aptidão e habilidade para lidar com uma ampla gama de questões técnicas”*.

53. De acordo com o item 3.17. da versão brasileira da norma, ABNT NBR ISO/IEC 27037.

54. Item 5.3.3. da ISO 27037.

Incidentes de segurança com dados pessoais em serviços de armazenamento em nuvem
do incidente. Este processo é importante para centralizar recursos e esforços na coleta de informações que realmente contribuirão para a investigação.

O tópico 6.1, “*Cadeia de Custódia*”, esclarece que o registro da cadeia de custódia deve conter, no mínimo, as seguintes informações: a) Identificador único de evidências; b) Quem acessou as provas e a hora e local em que ocorreram; c) Quem verificou a entrada e saída das evidências do local de preservação de evidências e quando isso aconteceu; d) Por que as evidências foram verificadas (qual caso e a finalidade) e a autoridade competente, se for o caso; e e) Quaisquer alterações inevitáveis na potencial evidência digital, bem como no nome do indivíduo responsável e a justificação para a introdução desta alteração.

Considerando o recorte proposto para este trabalho, destaca-se que há contextos em que a evidência digital é adquirida diretamente dos provedores de serviços em nuvem. Nestes casos, a NIST IR 8387⁵⁵ em seu item “3.2 1) e” alerta que pode não haver registro do item em um sistema de Gerenciamento de Evidências, assim “*as Unidades de Evidências Digitais precisarão ter um método para registrar as evidências que entram diretamente na unidade*”.⁵⁶

As evidências coletadas devem ser armazenadas de forma segura para evitar qualquer comprometimento, como alteração, perda ou acesso não autorizado. O uso de criptografia para proteger os dados armazenados é uma prática altamente recomendada. Esse ambiente deve ser isolado e seguro, utilizando preferencialmente ferramentas forenses que permitem a análise em modo somente leitura. A importância central da utilização destes instrumentos concentra-se no fato de que

55. O NIST IR 8387, também conhecido como “Draft NISTIR 8387: Considerações para Detecção e Análise de Ataques Cibernéticos em Rede”, é um documento do National Institute of Standards and Technology (NIST) dos Estados Unidos. Este documento fornece orientações sobre como as organizações podem detectar e analisar ataques cibernéticos em redes, abordando metodologias e técnicas para melhorar a postura de segurança cibernética das organizações. Ele apresenta diretrizes sobre como coletar, analisar e interpretar dados de rede para identificar possíveis atividades maliciosas e responder a incidentes de segurança de maneira eficiente.

56. GUTTMAN, B., WHITE, D., Williams, S.; WALRAVEN, T. Digital Evidence Preservation: Considerations for Evidence Handlers, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD, [online], 2022. <https://doi.org/10.6028/NIST.IR.8387>, https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=933104. Acesso em 01.07. 2024.

permitem a extração de dados sem modificar o conteúdo ou a estrutura das evidências. Neste sentido, Mujahid ensina:

*“A forense em nuvem exige o uso de ferramentas e técnicas especializadas para enfrentar os desafios dos ambientes de computação em nuvem. Essas ferramentas auxiliam na aquisição de dados, preservação de evidências, análise e interpretação de artefatos específicos da nuvem”.*⁵⁷

A título exemplificativo, Barreto e Brasil alertam sobre os riscos de práticas corriqueiras que comprometem os princípios das evidências digitais e prejudicam sua credibilidade:

*“Quando for utilizada a tecla printscreen ou for feito um screenshot (foto da tela), copia-se a tela que está aparecendo no terminal, transformando-a em imagem, sem, entretanto, salvar os metadados que compõem esse conteúdo, perdendo informações importantes sobre este, como as propriedades de criação, localização geográfica, etc. Além do mais, com qualquer editor de imagens é possível modificar o conteúdo apresentado, eis que fora produzido unilateralmente”.*⁵⁸

Além disso, as evidências devem ser armazenadas em dispositivos ou sistemas que tenham controles de acesso rigorosos, sendo crucial controlar e registrar quem tem acesso às evidências digitais. Somente indivíduos autorizados e com necessidade comprovada devem ter acesso aos dados. Qualquer acesso ou manipulação das evidências deve ser registrado para manter um histórico completo das interações.

Se as evidências precisam ser transferidas para outra equipe ou autoridade, deve-se preparar um plano de transferência detalhado. Este pode ser um ponto de atenção na etapa de arquitetar a transferência em comunicações destinadas à ANPD, por exemplo. O anexo B da norma indica quais são os requisitos mínimos de documentação para transferência de evidências. Com base no anexo, a documentação de transferência deve conter no mínimo: a) nome e endereço da autoridade competente; b) uma declaração da autorização, formação e qualificações do DEFR; c) o objetivo do exame; d) quais ações foram realizadas; e) quem fez o quê

57. MUJAHID, Zafer. *Cloud Forensics: Investigating Security Incidents in Cloud Environments*. Lahore: Department of Computer Science, University of Garrison Lahore, 2023. p. 6.

58. BARRETO, Alessandro Gonçalves; BRASIL, Beatriz Silveira. *Manual de investigação cibernética: à luz do marco civil da internet*. Imprensa: Rio de Janeiro, Brasport, 2016. p 65.

Incidentes de segurança com dados pessoais em serviços de armazenamento em nuvem
e quando; f) a cadeia de custódia relativa à investigação específica; g) listagem descritiva de potenciais provas digitais e suportes de armazenamento digital recolhidos e adquiridos; e h) informações sobre quaisquer exames, testes ou investigações usadas para criar a cópia da prova.

Quando as evidências digitais são apresentadas em procedimentos legais, tais como os procedimentos administrativos sob competência da ANPD, é necessário preparar um relatório abrangente que inclua todos os detalhes da cadeia de custódia. Este relatório deve explicar como as evidências foram coletadas, preservadas, analisadas e transferidas, corroborando para sua admissibilidade. Mesmo após a apresentação à autoridade, a cadeia de custódia deve ser mantida até que todas as questões legais sejam resolvidas, resguardando as evidências e registrando qualquer acesso ou manipulação adicional.

Nota-se que a análise das evidências digitais deve seguir uma metodologia sistemática e rigorosa, utilizando técnicas forenses estabelecidas para examinar logs, arquivos, registros de rede e outras fontes de dados relevantes. Os resultados da análise devem ser documentados de forma metodologicamente determinada, descrevendo os métodos utilizados, as evidências encontradas, e qualquer interpretação ou conclusão derivada dos dados. Essa documentação é importante para que os resultados possam ser verificados e considerados em diferentes contextos, incluindo os processos administrativos sob competência da ANPD, especialmente na composição do relatório de tratamento do incidente.

3. DEVERES DE COMUNICAÇÃO EM INCIDENTES DE SEGURANÇA COM DADOS PESSOAIS

Em abril de 2024, a ANPD publicou o Regulamento de Comunicação de Incidente de Segurança, estabelecendo critérios e prazos para comunicações à ANPD e aos titulares dos dados afetados. O Regulamento prevê a obrigação da elaboração do “relatório de tratamento de incidente” para o qual as evidências digitais podem ser especialmente úteis. O Relatório é definido no artigo 3º, inciso XIX como *“documento fornecido pelo controlador que contém cópias, em meio físico ou digital, de dados e informações relevantes para descrever o incidente e as providências adotadas para reverter ou mitigar os seus efeitos”*.

3.1. Categorização e comunicação entre agentes de tratamento

A comunicação entre agentes de tratamento, apesar de possuir recorte distinto do enfoque principal deste trabalho, possui pontos que merecem ser brevemente esclarecidos em prol de uma dinâmica holística em termos de comunicação. É recomendável que, diante de um incidente de segurança, a instituição afetada tenha clareza de qual é o seu enquadramento enquanto agente de tratamento.

Considerando melhores práticas contratuais em termos de privacidade e proteção de dados pessoais, esta categorização deve estar expressa nos contratos cujos dados pessoais tratados em decorrência de sua execução foram comprometidos. Caso isso não esteja expresso, caberá a interpretação conforme definições elencadas no art. 5º, incisos VI e VII da LGPD. Cabe ressaltar que as comunicações destinadas aos titulares e à ANPD, são aplicáveis aos Controladores de dados pessoais, nos termos do art. 4º do Regulamento.

Inobstante à atribuição dos principais deveres de comunicação aos Controladores, cláusulas de proteção de dados frequentemente prevêm obrigações a serem observadas também por Operadores, como: i) um prazo de pouquíssimos dias, ou até mesmo horas, para a comunicação do incidente ao Controlador; ii) um ponto de contato específico no Controlador para comunicações referentes a incidentes de segurança, visando a otimização da adoção de medidas emergenciais e mitigação de danos reputacionais; e iii) obrigações de suporte e colaboração na apuração do incidente, bem como a produção de relatórios.

Em decorrência deste último item a adequada condução de investigações cibernéticas, é imprescindível tanto para Controladores, quanto para Operadores de dados pessoais, bem como para subcontratados que eventualmente atuem em seu nome. Conforme explanado ao longo deste artigo, a eficiência da condução investigativa demanda conhecimentos multidisciplinares legais, regulatórios e referentes à tecnologia da informação.

3.2. Comunicação à Autoridade Nacional de Proteção de Dados

Nos termos do art. 6º do Regulamento, a comunicação à ANPD deve ser feita pelo Controlador no prazo máximo de 03 dias úteis, e poderá ser complementada em até 20 dias úteis. Ressalva-se que nos termos do Art. 14, II do Regulamento de aplicação da LGPD para agentes de tratamento de pequeno porte, estes prazos são contados em dobro.⁵⁹ A LGPD, em seu art. 48, limita o dever de comunicação aos incidentes que possam causar riscos ou danos relevantes aos titulares.

No processo administrativo contra a Secretaria de Assistência Social, Combate à Fome e Políticas sobre Drogas (“SAS”)⁶⁰, a Autoridade determinou que a Controladora complementasse a comunicação de incidente de segurança, colacionando ao processo o *“relatório de tratamento de incidente incluindo os seguintes detalhes: registros de acessos dos servidores que armazenavam a base de dados comprometida e a causa-raiz do incidente.”*⁶¹ O Despacho 0042417 indicou a insuficiência de *“itens que deveriam compor o relatório de tratamento do incidente”*, entre elas, *“a ausência de indicativos de acessos indevidos por meio da própria aplicação web; a falta de esclarecimento da cronologia do incidente”* (grifou-se).

Nota-se que os registros de acesso à aplicação, conceituados pelo art. 5º, VIII do MCI como *“conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP”*, possuiriam expressivo potencial de contribuição para comunicações consideradas adequadas pela Autoridade. Isto é, se prestariam tanto compor indicativos de acessos indevidos, quanto seus metadados de data e hora do acesso se prestariam a compor o mencionado *“esclarecimento da cronologia do incidente”*.

59. BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). *Resolução ANPD nº 2, de 27 de janeiro de 2022*. Disponível em: <https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019>. Acesso em: 2 jul. 2024.

60. Auto de Infração nº 11/2022/CGF/ANPD (0050468). Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/ri-pas-pe-versao-publica.pdf>. Acesso em: 03.05.2024

61. Ibidem.

3.3. Comunicação aos titulares

Nos termos do art. 9º do Regulamento, a comunicação aos titulares envolvidos deve ser realizada pelo Controlador no prazo máximo de 03 dias úteis, observada a contagem em dobro para agentes de tratamento de pequeno porte.⁶² É importante observar, também, que conforme o art. 9º, § 1º, a comunicação aos titulares deverá utilizar fazer uso de linguagem acessível, além de ocorrer de forma direta e individualizada⁶³, caso seja viável identificá-los. Nota-se que as evidências digitais, cuja interpretação muitas vezes demanda conhecimento técnico, geralmente não possuem alta relevância no conteúdo das comunicações direcionadas aos titulares, mas podem ser cruciais para direcioná-las a partir da identificação dos dados comprometidos e, conseqüentemente, dos indivíduos afetados.

CONCLUSÃO

Um contexto contemporâneo de ascensão da utilização de serviços de armazenamento em nuvem, bem como de ataques cibernéticos em todo o mundo, evidencia a necessidade de compreender medidas técnicas e jurídicas que possam guiar respostas adequadas em contextos de incidentes de segurança nestes ambientes. Entende-se que a investigação cibernética e a preservação de evidências digitais figuram como elementos essenciais para que as comunicações decorrentes do incidente sejam bem sucedidas, cumprindo disposições legais, regulatórias e contratuais.

Assim, caso haja um incidente de segurança no *cloud storage* de uma organização, é possível realizar a solicitação dos registros de acesso, enquanto evidências digitais, aos *Cloud Service Providers*. Conforme discutido, “*acesso a logs, dados e cooperação dos provedores de nuvem em investigações são cruciais para uma resposta eficaz a*

62. BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). Resolução ANPD nº 2, de 27 de janeiro de 2022. Disponível em: <https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019>. Acesso em: 2 jul. 2024

63. O § 2º do mesmo artigo prevê que “*idera-se comunicação de forma direta e individualizada aquela realizada pelos meios usualmente utilizados pelo controlador para contatar o titular, tais como telefone, e-mail, mensagem eletrônica ou carta.*”.

Incidentes de segurança com dados pessoais em serviços de armazenamento em nuvem incidentes e coleta de evidências⁶⁴. Assim, a obtenção e interpretação dessas informações assume um papel central na investigação do incidente, bem como no suporte aos deveres de comunicação conexos, especialmente no que tange ao relatório de tratamento de incidente destinado à ANPD. Desta forma, buscou-se esclarecer pontos importantes a serem considerados em prol de uma dinâmica eficiente no compartilhamento de evidências entre os CSPs e as organizações.

Demonstrou-se, também, questões metodológicas a serem observadas na cadeia de custódia das evidências digitais. Seguir rigorosamente *frameworks* aplicáveis consolidados é essencial para assegurar a integridade, a autenticidade e a admissibilidade das evidências digitais. Ao adotar diretrizes como as orientadas pela ISO/IEC 27037:2013, as organizações podem aumentar a confiabilidade de suas investigações cibernéticas e garantir que as evidências digitais sejam aceitas em procedimentos legais e administrativos. Assim, integrando sistematicamente os pontos abordados, o presente artigo buscou esclarecer pontos aptos a guiarem medidas empresariais emergenciais na gestão de incidentes de segurança, mitigando os respectivos danos patrimoniais e reputacionais decorrentes.

REFERÊNCIAS

- ABNT. NBR ISO/IEC 27037: *Diretrizes para identificação, coleta, aquisição e preservação de evidência digital*. Rio de Janeiro, 2013.
- ASHAWA, Moses & Mansour, Ali & Riley, Jackie & Osamor, Jude & Owoh, Nsikak. *Digital Forensics Challenges in Cyberspace: Overcoming Legitimacy and Privacy Issues Through Modularisation*. Cloud Computing and Data Science, 2023. 140-156. 10.37256/ccds.5120233845.
- ASSOCIAÇÃO AMERICANA DE ADVOGADOS. *Evidence Preservation*. Disponível em: https://www.americanbar.org/groups/tort_trial_insurance_practice/committees/cyber-data-privacy/evidence-preservation/. Acesso em: 3 jul. 2024.
- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27037:2013 - *Tecnologia da Informação - Técnicas de Segurança - Diretrizes para identificação, coleta, aquisição e preservação de evidência digital*. Rio de Janeiro, 2013.
- Autoridade Nacional de Proteção de Dados. Coordenação-Geral de Fiscalização. Coordenação de Fiscalização. *RELATÓRIO DE INSTRUÇÃO Nº 3/2024/FIS/CGF - VERSÃO PÚBLICA*.

64. MUJAHID, Zafer. *Cloud Forensics: Investigating Security Incidents in Cloud Environments*. Lahore: Department of Computer Science, University of Garrison Lahore, 2023. p. 5-6.

- Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/ri-pas-pe-versao-publica.pdf>. Acesso em: 30 jun. 2024.
- BARRETO, Alessandro Gonçalves; BRASIL, Beatriz Silveira. *Manual de investigação cibernética: à luz do marco civil da internet*. Imprensa: Rio de Janeiro, Brasport, 2016.
- BARROSO, Carolina Rodrigues de Carvalho. *Meios de investigação e produção de provas nos crimes cibernéticos*. Universidade Federal Fluminense, Niterói, 2019.
- BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). *Resolução ANPD nº 2, de 27 de janeiro de 2022*. Disponível em: <https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019>. Acesso em: 2 jul. 2024
- BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). *Resolução ANPD nº 15, de 24 de abril de 2024*. Disponível em: <https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024>. Acesso em: 2 jul. 2024.
- BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 3 jul. 2024.
- BRASIL. *Convenção sobre Cibercrime*. Budapeste: MPF, 2001.
- BRASIL. Decreto nº 11.491, de 12 de abril de 2023. Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001. *Diário Oficial [da] República Federativa do Brasil*, Poder Executivo, Brasília, DF, 13 abr. 2023.
- BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. *Diário Oficial [da República Federativa do Brasil]*, Poder Legislativo, Brasília, DF, 23 abr. 2014. Disponível em: http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2014/Lei/L12965.htm. Acesso em: 30 jun. 2024.
- BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2020]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14020.htm. Acesso em: 30 jun. 2024.
- Brasil. Lei nº 13.964, de 24 de dezembro de 2019. Institui o "Pacote Anticrime". *Diário Oficial da União*, Brasília, DF, 26 dez. 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13964.htm. Acesso em: 3 jul. 2024.
- BRASIL. Superior Tribunal de Justiça. *Recurso Especial 1.784.156/SP*. Relator: Min. Ricardo Villas Bôas Cueva. Julgado em 14/08/2019. *Diário da Justiça Eletrônico*, 21/11/2019.
- Canaltech. *Ataques contra a nuvem aumentaram 48% em 2022*. Disponível em: <https://canaltech.com.br/seguranca/ataques-contra-a-nuvem-aumentaram-48-em-2022-242120/>. Acesso em: 3 mai. 2024.

- Incidentes de segurança com dados pessoais em serviços de armazenamento em nuvem
- CEROY, Frederico Meinberg. *Os conceitos de provedores do Marco Civil da Internet*. Set. 2014. JusNavigandi. Disponível em: <https://jus.com.br/artigos/31938/os-conceitos-de-provedores-no-marco-civil-da-internet#google_vignette>. Acesso em: 9 mar. 2016.
- Chung, J. Park, S. Lee, and C. Kang. *Digital forensic investigation of cloud storage services*. Digital Invest. 9, 2, 2012, 81–95.
- Conteúdo Jurídico. *Cadeia de custódia da prova na investigação criminal em ambiente digital*. Disponível em: <https://conteudojuridico.com.br/consulta/Artigos/58599/cadeia-de-custodia-da-prova-na-investigao-criminal-em-ambiente-digital>. Acesso em: 2 jul. 2024.
- DA SILVA, Rosane Leal; DALLA FAVERA, Rafaela Bolson; DE QUADROS OLMOS, Olívia Martins. *A responsabilidade civil dos principais cloud computing providers em razão da perda de arquivos*. Revista da Faculdade de Direito UFPR, 2018, 63.2: 89-113.
- EASWARAMOORTHY, S.; THAMBURASA, S.; SAMY, G.; BHUSHAN, S. B.; ARAVIND, K. *Digital forensic evidence collection of cloud storage data for investigation*. In: INTERNATIONAL CONFERENCE ON RECENT TRENDS IN INFORMATION TECHNOLOGY (ICRTIT), 2016, Chennai. Anais [...]. Chennai: IEEE, 2016. p. 1-6. doi: 10.1109/ICRTIT.2016.7569516.
- GUTTMAN, B. , WHITE, D. , WILLIAMS, S. and WALRAVEN, T. *Digital Evidence Preservation: Considerations for Evidence Handlers*, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD, [online], 2022. <https://doi.org/10.6028/NIST.IR.8387>, https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=933104. Acesso em 01.07. 2024.
- HEISER, Jay. *What You Need to Know About Cloud Computing Security and Compliance*. Disponível em: Acesso em: 30 jun. 2024.
- IFTO - Instituto Federal de Educação, Ciência e Tecnologia do Tocantins. *Política de Gestão da Segurança da Informação (PGISI)*. Disponível em:<https://portal.iftto.edu.br/acesso-a-informacao/seguranca-da-informacao/documentos-lgpd-iftto/PGISI.pdf>. Acesso em: 03 mai. 2024
- INSTITUTO DE REFERÊNCIA EM INTERNET E SOCIEDADE (Brasil) (Org.). *Portas lógicas e registros de acesso: das possibilidades técnicas aos entendimentos dos tribunais brasileiros*. Belo Horizonte: Iris, 2017. Disponível em: https://irisbh.com.br/wp-content/uploads/2017/11/Portas-L%F3gicas-e-Registros-de-Acesso_PT.pdf. Acesso em: 05 jun. 2024
- MACHADO, Leonardo Marcondes. *Aplicação da cadeia de custódia da prova digital*. Revista Consultor Jurídico, 2020. 6p. Disponível em: <https://www.conjur.com.br/2020-mar-31/academiapolicia-aplicacao-cadeia-custodia-prova-digital>. Acesso em: 2 jul. 2024.
- MALIK, Annas Wasim *et al.* *Cloud digital forensics: beyond tools, techniques, and challenges*. Sensors, Basel, v. 24, n. 2, p. 433, 2024. Disponível em: <https://doi.org/10.3390/s24020433>. Acesso em: 2 jul. 2024.

- MUJAHID, Zafer. *Cloud Forensics: Investigating Security Incidents in Cloud Environments*. Lahore: Department of Computer Science, University of Garrison Lahore, 2023.
- NETO, M. F.; SANTOS, J. E. L. d. *Apontamentos sobre a cadeia de custódia da prova digital no Brasil*. Em Tempo, v. 20, 2020.
- PEGORARO DE ARAUJO, C. V. *Os Aspectos Gerais Dos Tratados Internacionais e a Convenção de Budapeste Sobre Crimes Cibernéticos*. Revista Da Faculdade De Direito Da Universidade Federal De Uberlândia, 50(1), 2022, 145–165. <https://doi.org/10.14393/RFADIR-50.1.2022.65259.145-165>.
- RAGHAVENDRA, S. *et al. Critical retrospection of security implication in cloud computing and its forensic applications*. Security and Communication Networks, v. 2022, artigo 1791491, 2022. Disponível em: <https://doi.org/10.1155/2022/1791491>. Acesso em: 2 jul. 2024.
- SURANGE, G.; KHATRI, P. *IoT forensics: A review on current trends, approaches and foreseen challenges*. In: Proceedings of the 2021 8th International Conference on Computing for Sustainable Global Development (INDIACom), 17-19 March 2021, New Delhi, India. Piscataway: IEEE, 2021. p. 909-913.
- VEBER, Jaromír; SMUTNY, Zdenek. *Standard ISO 27037:2012 and Collection of Digital Evidence: Experience in the Czech Republic*. European Conference on Information Warfare and Security, EC-CWS. 2015. 294-299.

III

NEUTRALIDADE DA REDE

10 ANOS DO MARCO CIVIL DA INTERNET:

BREVES REFLEXÕES SOBRE NEUTRALIDADE DA REDE

Giovanni Simão Triginelli

Mestrando na Faculdade de Direito da Universidade Federal de Minas Gerais.
Graduado em Direito pela Faculdade de Direito da Universidade Federal de Minas
Gerais. Advogado.

DOI: <https://doi.org/10.59224/dti7.ch4>

Resumo: A publicação do Marco Civil da Internet foi um marco histórico brasileiro e instigou países internacionais a fazerem o mesmo. Fruto de um amplo debate democrático, o Marco Civil da Internet arrolou princípios basilares para uma manutenção de uma internet harmoniosa e capaz de preservar os direitos humanos ao passo que buscou a proteção dos modelos de negócios e inovação. A neutralidade de rede surge como um dos pilares deste cenário, por buscar uma transmissão de dados isonômica e sem discriminação quanto a origem, destino, conteúdo, serviço, terminal ou aplicação. Todavia, ultrapassados uma década da vigência da referida lei é necessário revisitar o ecossistema para verificar, mesmo que brevemente, o cenário que se encontra e quais são os desafios enfrentados durante esse período.

Palavras-chave: Marco Civil da Internet. Neutralidade de Rede. *Fair Share*.

Abstract: *The publication of the Marco Civil da Internet was a historic milestone and prompted international countries to do the same. The result of a broad democratic debate, the Marco Civil da Internet listed basic principles for maintaining a harmonious internet capable of preserving human rights, while seeking to protect business models and innovation. Net neutrality emerges as one of the pillars of this scenario, as it seeks an isonomic data transmission without discrimination as to origin, destination, content, service, terminal or application. However, a decade after the law came into force, it is necessary to revisit the ecosystem to see, albeit briefly, the current scenario and the challenges faced during this period.*

Keywords: *Internet Civil Rights Framework. Network Neutrality. Fair Share.*

SUMÁRIO: 1. Introdução. 2. Neutralidade de Rede. 2.1 Breve Relato Histórico. 2.2 Análise histórica da neutralidade de rede no Brasil 2.3 Modalidades de discriminação 2.3.1 Hipóteses Legais 2.3.2 *Zero Rating* 2.3.3 *Fair Share* 3. Conclusão. Referências.

1. INTRODUÇÃO

O Marco Civil da Internet foi, sem dúvidas, um ponto de destaque legislativo nacional. Iniciado como uma resposta a onda de crimes cibernéticos que se difundia no Brasil e no Mundo¹, teve seu formato incipiente como o de uma lei penal, mas foi posteriormente transmutada em lei civil após a reação pública da sociedade quanto ao formato inicial².

Para a sua construção normativa, organizou-se uma consulta pública pela internet, dividida em duas etapas. Na primeira etapa apresentou-se um texto inicial com conteúdo limitado à princípios que regulamentariam a internet. Durante os 45 dias seguintes interessados no tema detalharam os princípios e propuseram novos temas correlacionados para possível inserção na lei que, posteriormente foi compilado pela comissão nomeada pelo Ministério da Justiça em um anteprojeto.

O anteprojeto continha temas relevantes para a edição de uma futura lei e foi o texto base para uma primeira minuta levada em seguida à consideração, novamente, da sociedade brasileira. Mais uma vez, a plataforma virtual foi aberta para que qualquer interessado pudesse expressar a sua opinião sobre a redação proposta, sendo

1. “A neutralidade de rede, inclusive, foi um dos pontos mais polêmicos do Marco Civil da Internet, tendo sido discutida durante toda a tramitação legislativa. Estima-se que se não fosse pelo escândalo de interceptação das comunicações eletrônicas de diversos Estados, por parte do Governo dos Estados Unidos da América (conhecido como caso Edward Snowden), talvez até hoje o Marco Civil não houvesse sido aprovado no Congresso Nacional. Principalmente porque a prioridade, nos anos seguintes, passou a ser a grave crise econômica e política que se instalou no país.” PARENTONI, Leonardo. *Neutralidade da Rede: Mudanças na Infraestrutura da internet e como isso influencia na sua vida*. In: Revista Jurídica da Presidência. Janeiro de 2018, pág 584
2. “O Marco Civil foi criado como parte de uma reação pública forte contra um projeto de lei sobre crimes cometidos através da Internet no Brasil. O PL nº 84/99, de autoria do Deputado Luiz Piauhyllino, recebeu um substitutivo do Senador Eduardo Azeredo que culminou com a associação do Senador (e posteriormente Deputado) com o destino do projeto. A partir de 2007, o projeto de lei passou até mesmo a ser apelidado de “Lei Azeredo” Com um alcance tão amplo (que se aproximava das discussões sobre os projetos de lei SOPA e PIPA nos Estados Unidos), o projeto de lei teria transformado em criminosos milhões de usuários de Internet no Brasil. Mais ainda, ele teria restringido oportunidades de inovação, lançando à ilegalidade práticas necessárias para atividades típicas de pesquisa e desenvolvimento.” SOUZA, Carlos Affonso; LEMOS, Ronaldo. *Marco Civil da Internet: construção e aplicação*. Editar Editora. Juiz de Fora, 2016. Pág. 17

facultado ainda sugerir alterações que pudessem aperfeiçoar o texto sugerido³.

A participação de diversos setores da sociedade, empresas nacionais e estrangeiras, associações e pessoas diretamente interessadas ao bom uso da internet foi um fato inédito no Brasil e fundamentou, inclusive, pesquisas públicas posteriores direcionadas a uma participação mais democrática na construção legislativa nacional. Ademais, trouxe mais legitimidade e segurança quanto ao seu conteúdo, apesar do resultado legal ter se constituído como resultado de opiniões e valores aparentemente antagônicos.

O Marco Civil da Internet foi, portanto, uma norma inovadora e capaz de promover as liberdades individuais, proteger os direitos humanos e proporcionar a livre concorrência. A lei trouxe a mensagem de uma internet aberta e colaborativa para a construção de um ecossistema harmonioso e adequado para preservar temas como a privacidade, liberdade de expressão, direito à associação e reunião, acesso à cultura, inovação e educação. Não é à toa que serviu de inspiração para outros países regulamentar a internet⁴.

Neste ambiente complexo com atuação simultânea de vários atores, como operadoras de telecomunicações, provedores de acesso, provedores de informação, serviços e aplicações, além de usuários, por vezes, com interesses conflitantes, a neutralidade⁵ vem a ser uma característica a ser buscada em todas as camadas que

3. SOUZA, Carlos Affonso; LEMOS, Ronaldo. *Marco Civil da Internet: construção e aplicação*. Editar Editora. Juiz de Fora, 2016. Pág. 20

4. “Uma vez aprovado em 2014, o Marco Civil serviu de inspiração para um processo de construção colaborativa de uma Declaração de Direitos para Internet, realizada pelo governo italiano. Citando expressamente a experiência brasileira e convidando diversos atores envolvidos com o Marco Civil para apresentar as suas contribuições ao Parlamento Italiano, a cooperação entre os dois países demonstra o rápido impacto que a aprovação do texto brasileiro desencadeou.” SOUZA, Carlos Affonso; LEMOS, Ronaldo. *Marco Civil da Internet: construção e aplicação*. Editar Editora. Juiz de Fora, 2016. Pág. 32

5. Uma forma possível de abordar, ao menos parcialmente, a complexa semântica da expressão “a internet deve ser neutra” é fazer analogia a um princípio técnico básico, que sempre inspirou a rede. A internet foi concebida como sendo primariamente uma rede “fim a fim” (*end to end*). Nela os pacotes de dados, iniciados num ponto da borda da rede e destinados a outro ponto, não devem sofrer nenhum a interferência indevida GETSCHKO, DEMI. *As origens do Marco da Internet*. In: Marco civil da Internet. Coordenadores: LEMOS, Ronaldo; LEITE, George Salomão Leite. Editora

conjuntamente formam a Internet.

A neutralidade de rede surge como um dos principais princípios positivados na lei, na medida em que busca garantir a isonomia do tráfego de dados da internet, sem discriminação ou privilégios injustificados por parte dos provedores de internet. Além do cunho histórico, a neutralidade de rede busca garantir a todos os usuários que tenham acesso, uma internet livre, aberta e não discriminatória.

A leitura inicial do princípio nos induz a acreditar que a obviedade da neutralidade da rede não enfrenta desafios adversos. No entanto, as práticas mercadológicas têm se dedicado, direta ou indiretamente, pelas mais variadas formas, a burlá-lo ou ignorá-lo, sempre com objetivos obscuros ou desvirtuados do bom funcionamento da internet, destacando-se, o *zero rating* e mais recentemente o *fair share*.

Este artigo busca então trazer breves reflexões sobre a neutralidade da rede e seu funcionamento após o transcurso do prazo de dez anos da vigência do Marco Civil da Internet. No primeiro momento, traçar-se-á um panorama sobre a neutralidade da rede, com breve relato histórico, indicação de conceitos importantes e os benefícios obtidos com o seu respeito. Posteriormente, analisar-se-á as principais práticas mercadológicas, que possam, direta ou indiretamente, afetar a neutralidade da rede, em especial o *zero rating* e o *fair share*. Em seguida, tecerá breves reflexões sobre o cenário atual obtidas com esse breve ensaio e expectativas para os próximos anos.

2. NEUTRALIDADE DE REDE

2.1. Breve relato histórico

O princípio da neutralidade está umbilicalmente ligado à própria arquitetura originária da internet, criada para ser um meio de comunicação seguro, rápido e disponível mesmo que um dos seus componentes fossem danificados.

Para que isso fosse possível, aplicou-se na criação da internet quatro princípios fundamentais, quais sejam: a) comutação de pacotes (*packet switching*); b) modularidade (*modularity*); c) camadas de rede (*network layers*); e, d) execução de aplicações em camada superior (*end-to-end*).

A comutação de pacotes tem como característica básica a transmissão de pacotes de dados devidamente divididos, a fim de sejam separadamente transmitidos. Até aqui, algo semelhante ao correio tradicional, em papel. A grande diferença é que os vários pacotes podem trafegar simultaneamente, por rotas diversas, inclusive mudando de trajeto durante o percurso, para privilegiar aquele que for mais rápido e eficaz (*switching*)⁶.

A modularidade dispõe que a internet seja construída com a conjunção de vários componentes, independentes um dos outros, de forma a reduzir, ao máximo a dependência da rede sobre cada um deles. A grande vantagem da modularidade é possibilitar aprimoramentos internos em cada componente da rede sem que para isto seja preciso alterar sua infraestrutura como um todo.⁷

As camadas de rede seguem o mesmo parâmetro divisório dos princípios acima, arquitetando-se verticalmente para processamento da comunicação dos dados via internet. Em breve síntese, a transmissão de dados se inicia na camada física ou equipamentos físicos (ex. *smartphones*), individualizados por um protocolo IP, que acessa a camada de conexão, remetendo-se os pacotes de dados fragmentados, devidamente reagrupados ao chegar nas aplicações como destino final localizadas na camada superior da internet⁸.

6. PARENTONI, Leonardo. *Neutralidade da Rede: Mudanças na Infraestrutura da internet e como isso influencia na sua vida*. In: Revista Jurídica da Presidência. Janeiro de 2018.

7. “Para lograr isso, todo módulo possui dois tipos de informação, a visível e a invisível (TANENBAUM; WETHERALL, 2011, p. 29). Informação visível é aquela que qualquer componente da rede precisa conhecer para se conectar com determinado módulo. Ela deve permanecer inalterada e disponível a qualquer interessado, durante toda a vida da rede, para não prejudicar a comunicação entre os módulos. (...) Diversamente, a informação necessária para o funcionamento interno de cada módulo é chamada de informação invisível. Ela normalmente é conhecida apenas pelo fabricante do módulo, consubstanciando sua vantagem competitiva em relação aos concorrentes. Por exemplo, a resolução e a forma de funcionamento do monitor.” PARENTONI, Leonardo. *Neutralidade da Rede: Mudanças na Infraestrutura da internet e como isso influencia na sua vida*. In: Revista Jurídica da Presidência. Janeiro de 2018, pág. 567.

8. “Na verdade, os dados primeiro fluem de cima para baixo, do dispositivo utilizado pelo usuário para gerar os dados, passando pelo TCP/IP, que irá individualizá-los, roteá-los e fracioná-los em pacotes, até que atinjam a camada física. Daí por diante, serão transmitidos em sua forma bruta até alcançarem o local em que se situa o dispositivo de destino. Feito isso, passam a fluir de baixo

Não obstante esse caráter arquitetônico, com a evolução da internet, se percebeu uma grande disputa concorrencial entre as empresas de telefonia, como herdeiras da grande infraestrutura, para abocanhar fatias significativas desse novo mercado e desestimular a entrada de novos *players*.

À época, cogitou-se que se realizasse uma abertura integral do sistema de conexão a todos os interessados, almejando-se estimular uma pulverização do mercado (*open access*). Logicamente não foi o caminho adotado – talvez aqui pelo intenso lobby das empresas de telefonia – considerando serem medidas contra produtivas e contrárias até à própria estrutura arquitetônica da internet que mantinha o poder decisório em suas pontas. Por isso, optou-se, por estimular uma competição entre os provedores de conteúdo através de um regime específico que garantisse aos usuários o direito de usar livremente aplicações, focando apenas na qualidade do conteúdo⁹.

A adoção do entendimento acima trouxe um grande desestímulo aos investimentos em infraestrutura da internet aliado a um grande cenário de integração vertical entre as empresas detentoras do arcabouço estrutural, mediante a utilização do poder dominante as empresas de telecomunicações para discriminar provedores não

para cima, indo da camada física para a de conexão, passando pelo TCP/IP, que se encarregará de conferir se a destinação está correta e, em caso afirmativo, reagrupar os pacotes, reconstituindo os dados originais para, em seguida, transmiti-los à aplicação que irá processá-los (em linguagem de programação), até que o resultado final seja exibido no dispositivo de destino. PARENTONI, Leonardo. *Neutralidade da Rede: Mudanças na Infraestrutura da internet e como isso influencia na sua vida*. In: Revista Jurídica da Presidência. Janeiro de 2018, pág. 570

9. “The goal of this paper was to make an initial case for a broadband discrimination regime as an alternative to the structural remedy of open access to achieve the goal of network neutrality. At this point, the newness of the concept means much unavoidable vagueness as to its operation. It is easier to point out examples of application discrimination that seem unjustified than to elucidate a standard that nearly separates the legitimate from the suspect. For example, there remains much work to better define what the concepts of network neutrality and discrimination would fully entail as a regulatory matter, or even as a regulatory threat. Should neutrality be defined by IETF standards? The intuitions of network theorists? Government definition? Any workable regime designed to achieve network neutrality will need a more precise conception of this and other matters. Nonetheless, the hope is that the general framework described here might serve to begin the effort to discourage the most blatant or thoughtless disfavoring of certain application types through network design. WU, Tim. *Network neutrality, broadband discrimination*. J. on Telecomm. & High Tech. L., v. 2, p. 141, 2003

afiliados. Foi nesta época que ocorreu o clássico *case* da Madison River Communications¹⁰.

A falha de mercado e o risco concorrencial são fortes elementos para se constituir uma regulação normativa direcionada a impor limites, regular atuações dos envolvidos e proteger direitos humanos e econômicos correlatos. Nesta época, cogitou-se um novo viés da neutralidade da rede, qual seja, neutralidade regulatória¹¹, sabidamente rechaçada ante a impossibilidade do Estado se manter alheio as nuances do mercado.

Em que pese as várias discussões e teoremas propostos, a celeuma da discussão sobre neutralidade da rede se limitou a duas visões aparentemente antagônicas: de um lado a proteção ao sistema de mercado e política concorrencial e do outro o entendimento da neutralidade de rede como meio de promoção dos direitos humanos e democracia.

Aqueles que defendem a visão mercadológica da neutralidade de rede se baseiam em dois interesses essencialmente encrustados no modelo capitalista e no direito de propriedade, quais sejam (i) direito de usar o ativo da melhor forma que lhe aprouver; (ii) direito de excluir terceiros de usar o ativo.

Segundo tais defensores, o objetivo fundamental da defesa desses direitos é criar condições para a maximização da riqueza na sociedade. Primeiro ao permitir que o proprietário utilize do ativo da forma que bem entender, espera-se que aquele direcione os seus esforços para o uso que gerar o maior valor possível do produto, atraindo-se investimentos. Segundo ao excluir terceiros do uso do ativo, o proprietário é capaz de evitar o problema da chamada “tragédia dos comuns”, a qual constitui a tendência de um recurso ou ativo cujo acesso seja irrestrito ser explorado de

10. A Federal Communications Commission (FCC) multou a Madison River Communication, da Carolina do Norte, em US\$ 15,000, no ano de 2005, por bloquear o tráfego de dados da Vonage que oferecia ligações de voz em VoIP, afetando os seus usuários. Em função desta multa, outras operadoras de conexão que também bloqueavam os mesmos tráfegos de dados, consentiram em desbloquear, como por exemplo, a Telco. Disponível em <https://www.cnet.com/home/internet/telco-agrees-to-stop-blocking-voip-calls/>. Acesso 15.06.24 às 19:44hs

11. Neste caso, a teoria se direcionava a evitar qualquer normatização sobre a neutralidade de rede, deixando ao mercado uma autorregulação.

forma excessiva¹².

Nesta linha argumentativa a neutralidade de rede compromete o sistema capitalista mercadológico, pois impede que se tome decisões empresariais visando uma melhor exploração do produto “rede” com a criação de produtos adequados a cada segmento de mercado e priorizar certos pacotes de dados em detrimento de outros. Ademais, impossibilita que se realize a cobrança por quantidade de dados transmitidos – e não por acesso à internet –, comprometendo diretamente na capacidade dos empresários em gerar maior valor e auferir lucros com seu ativo¹³. Como consequência lógica deste cenário, tem-se o baixo estímulo à investimentos e inovação e o comprometimento de se ofertar um melhor preço e produtos aos usuários finais.

Por outro lado, os defensores da neutralidade de rede como um meio de promoção dos direitos humanos trouxeram a carga uma internet como manifestação da liberdade de expressão, proteção à privacidade, acesso à educação, cultura. Neste viés interpretativo, almeja-se afastar o cenário de uma internet discriminatória, vigilante e capaz de impedir a livre escolha do usuário em acessar quaisquer tipos de conteúdo ou usufruir deste ecossistema como entender, culminando, em última análise em uma deterioração da democracia digital.

Dentre os principais argumentos desta linha defensiva destaca-se uma tendência discriminatória manifestada pela priorização de tráfego em benefício de alguns e prejuízo para outros usuários ou provedores de conteúdo. Corolário disso existe a construção de ofertas diferenciadas com a parametrização de preços em pacotes específicos para a certos segmentos culminando na exclusão daqueles que não podem arcar com tais valores. Criticam ainda a possibilidade de realização de acordos comerciais entre empresas com a finalidade de ampliação dos custos para os provedores de conteúdo, culminando, também, em uma medida discriminatória, principalmente aos provedores em estágio incipiente ou com menor alcance.

12. MARANHÃO, Juliano; MATTOS César. Neutralidade de Rede VS Neutralidade Regulatória. *Legal Grounds Institute*. São Paulo, 2024, pag. 36

13. “Por esse motivo, Christofer Yoo propunha um princípio oposto, que chamou de diversidade de rede, que permitiria diferentes abordagens para a gestão do tráfego por parte dos operadores, conforme tipo de demanda.” MARANHÃO, Juliano; MATTOS César. Neutralidade de Rede VS Neutralidade Regulatória. *Legal Grounds Institute*. São Paulo, 2024, pag. 20

Este último argumento tem sido mais adotado nas decisões governamentais, precipuamente pela base ideológica americana de destaque na autonomia privada, calcada, em específico, na ideia de que a escolha por conteúdo na internet deve ser absolutamente livre de qualquer constrangimento ou interesse comercial. O usuário, podendo acessar todas as opções de conteúdo disponíveis, deveria eleger aqueles apenas pela sua qualidade, e assim, manifestar livremente suas preferências além de suas opiniões nos canais e mídias digitais idênticas, em termos de qualidade de transmissão¹⁴.

Os provedores de acesso somente teriam ingerência quanto ao acesso à internet, não lhe recaindo qualquer possibilidade de diferenciação na transmissão de dados, mas, ao contrário, lhe recairiam o dever ativo de manter a transmissão de dados de forma igualitária independentemente do conteúdo, origem, destino, terminal ou serviço.

Aqui, rechaça-se a ideia de uma vigilância e inspeção dos dados ou conteúdos transmitidos dentro da internet, o que, fatalmente, resultaria em uma violação da privacidade, liberdade de proteção de dados dos usuários. Afinal, para além da análise de quais conteúdos devam ser inspecionados ou vigiados, debruça-se sobre qual o momento de análise e sobre a quem recairia a legitimidade em proceder este filtro. Esta reflexão nos países onde o sistema de telecomunicações é provido pelo Estado, a discussão ainda ganha uma tonalidade eminentemente política¹⁵.

Percebe-se que a neutralidade de rede estava guiada por dois princípios finalísticos fundamentais: o princípio de controle nas pontas da rede (*end-to-end*) e a transmissão baseada no melhor esforço (*best effort*). Esses dois princípios fazem com que a inteligência e a complexidade da rede se localizem em suas pontas, onde estão os

14. MARANHÃO, Juliano; MATTOS César. Neutralidade de Rede VS Neutralidade Regulatória. *Legal Grounds Institute*. São Paulo, 2024, pag. 34

15. “Essa dimensão política ganha ainda mais tonalidade quando se considera a possibilidade de provimento de serviços de telecomunicações pelo Estado, quando a neutralidade da rede passa a se apresentar como bandeira para proteger o usuário contra a censura estatal e a vigilância do tráfego por parte dos governos. Tal aspecto ganhou força especialmente no debate europeu, diante da tradição europeia de proteção de dados e o papel do Estado no provimento de serviços de telecomunicações.” MARANHÃO, Juliano; MATTOS César. *Neutralidade de Rede VS Neutralidade Regulatória*. Legal Grounds Institute. São Paulo, 2024, pág. 34

agentes comunicadores, e não no seu núcleo, ou seja, não na infraestrutura de transmissão¹⁶.

A neutralidade da rede se concentrou nos riscos concorrenciais, primeiro para a competição na infraestrutura e depois para os riscos de que um mercado oligopolizado na infraestrutura pudesse ameaçar a promessa de ampla competição no mercado de conteúdo e serviços na internet, o que se aliou a interesse em estimular o investimento naqueles mercados, mesmo comprometendo o custo de acesso à internet pelos usuários finais.

Atualmente há predileção por este novo formato conceitual da neutralidade de rede a que estamos convivendo, qual seja, um ambiente online, com liberdade para receber e transmitir informações, capacidade de livre acesso e compartilhamento de conteúdo, aplicações e serviços, utilizando o dispositivo conforme sua vontade, sem ser indevidamente discriminado no tráfego de internet¹⁷.

Retoma-se o caráter originário em que a internet foi concebida como uma plataforma agnóstica com relação ao conteúdo que pode ser transmitido e à finalidade para qual pode ser usado, permitindo que os usuários finais decidam livremente como utilizar seus aplicativos¹⁸.

16. Trata-se de infraestrutura oposta à configuração da telefonia, conforme a caracterização feita por Hatfield, Mitchell e Srinagesh. Ou seja, na telefonia tradicional, os terminais são “estúpidos” (dumb), sendo os roteadores (switchers) que controlam os fluxos de tráfego de voz. Já na internet, os softwares nas pontas (edges) das redes é que controlam o tráfego de tudo (voz e dados), enquanto a rede em si é relativamente “estúpida” (dumb) quando comparada ao sistema de telefonia convencional MARANHÃO, Juliano; MATTOS César. *Neutralidade de Rede VS Neutralidade Regulatória*. Legal Grounds Institute. São Paulo, 2024, pág. 15.

17. “Indeed, in the online environment, freedom to receive and impart information and ideas is directly reflected on user’s capability to freely access and share content, applications and services, using device of their choice, without being unduly influenced by discriminatory delivery of internet traffic.” (BELLI, Luca. *End-to-End, Net Neutrality and Human Rights*. In: *Net Neutrality Compendium*, Editora Springer, 2016, pág. 12)

18. BELLI, Luca; DE FILIPPI, Primavera. *Net Neutrality Compendium: Human Rights, Free Competition and the Future of the Internet*. New York: Springer, 2016, pag. 13

2.2 Análise histórica da neutralidade de rede no Brasil

A história da neutralidade de rede no Brasil tem sua incipiência manifestada bem antes da publicação do Marco Civil da Internet. Segundo Pedro Henrique Soares Ramos existem três grandes eixos que influenciaram diretamente na construção normativa do Marco Civil da Internet:

“No Marco Civil da Internet é possível identificar três diferentes eixos, que desempenharam um papel fundamental na construção da regra de neutralidade de rede prevista no art. 9º da Lei: um ambiente regulatório formado por leis, resoluções da Anatel e princípios gerais já contidos em outros diplomas; uma rede de interesses do governo, cuja atuação do Executivo (diretamente ou por meio da Anatel e do CGI.br) e do Legislativo que desempenhou um papel determinante; e grupos de interesse que se posicionaram durante todo o debate¹⁹.”

A primeira menção relevante do princípio da não discriminação pode ser encontrada na Norma 004/1995 do Ministério das Comunicações, publicada com o objetivo de regular o uso dos meios da rede pública de Telecomunicações para provimento e utilização de serviços de conexão à internet. O item 5.4 desta norma dispunha que as entidades exploradoras de serviços públicos de telecomunicações não discriminarão os diversos provedores de serviços de conexão à internet (“PSCI”) quando do provimento de meios da rede pública de telecomunicações para prestação de serviços de conexão à internet. Percebe-se, neste primeiro momento, que a não discriminação recaiu sobre os provedores de conexão entre si.

Em momento subsequente, a Lei 9472/97, que dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador, em cumprimento a Emenda Constitucional n. 8 de 1995²⁰, trouxe a proteção aos usuários de serviços de telecomunicações o direito de não serem discriminados quanto às

19. RAMOS, Pedro Henrique Soares. Arquitetura da rede e regulação: a neutralidade da rede no Brasil. Dissertação (Mestrado em Direito) - FGV - Fundação Getúlio Vargas, São Paulo, 2015. Pág. 64

20. A Emenda Constitucional n. 8 de 1995 alterou o inciso XI e a alínea “a” do inciso XII do artigo 21 da Constituição Federal para acabar com o monopólio estatal nos serviços de telecomunicações. Disponível em < https://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc08.htm>. Acesso em 01/07/2024 às 16:43hs

condições de acesso e fruição do serviço (art. 3º, III)²¹.

Pode-se perceber ainda outras disposições impeditivas à discriminação nas Resoluções 614/13 e 447/2007 todas da Anatel, seja, quanto à disponibilização do uso das redes de forma não discriminatória²², obrigação de fornecer serviço de acesso à internet em condições igualitárias aos usuários²³ ou obrigação de fornecer serviços a preços justos, equânimes e não discriminatórios²⁴.

A Anatel, inclusive, em outras oportunidades à época, se posicionou favoravelmente à neutralidade de rede, por exemplo, quando a agência emitiu um comunicado específico sobre o uso das aplicações VoIP, dispondo que contratos de prestação de Serviços de Comunicação Multimídia (“SCM”) não podem impor restrições à transmissão de nenhum tipo de sinal ou quando houve a fusão entre a Brasil Telecom e Telemar, em 2008²⁵.

O Comitê Gestor da Internet (“CGI”)²⁶, também contribuiu com grande relevância através da Resolução CGI.br/RES/2009/003/P, onde se arrolou os princípios para

21. Nos moldes da Norma 004/1995 dos Ministério das Comunicações, o acesso à internet é considerado um serviço de valor adicionado, conceituado no artigo 61 da Lei 9.472/97: “Art. 61 – Serviço de valor adicionado é a atividade que acrescenta, a um serviço de telecomunicações que lhe dá suporte e com qual não se confunde, novas utilidades relacionadas ao acesso, armazenamento, apresentação, movimentação ou recuperação de informações. § 1º Serviço de valor adicionado não constitui serviço de telecomunicações, classificando-se seu provedor como usuário do serviço de telecomunicações que lhe dá suporte, com os direitos e deveres inerentes a essa condição.”

22. Artigo, 7º e 8º da Resolução 614/2013 e artigo 60 da Resolução 477/2007.

23. Artigo 38, 47, VII e 56, III da Resolução 614/2013 e artigo 6º, II da Resolução 477/2007

24. Artigo 68 da Resolução 614/2013 e artigo 35 da Resolução 477/2007.

25. “A Anatel passou a se posicionar sobre o assunto a partir de 2005, quando a agência emitiu um comunicado específico sobre o uso de aplicações VoIP, dispondo que “contratos de prestação de SCM não podem impor restrições à transmissão de nenhum tipo de sinal. Preocupações sobre a neutralidade da rede também foram presentes na discussão sobre a fusão entre a Brasil Telecom e Telemar (atualmente Oi), em 2008.” RAMOS, Pedro Henrique Soares. *Arquitetura da rede e regulação: a neutralidade da rede no Brasil*. Dissertação (Mestrado em Direito) - FGV - Fundação Getúlio Vargas, São Paulo, 2015. Pág. 69

26. Criado pela Portaria Interministerial n. 147, dos Ministros das Comunicações e Ministro da Ciência e Tecnologia, publicada em 31 de maio de 1995 e atualmente regulamentado pelo Decreto n. 4.829, publicado em 03 de setembro de 2003, o Comitê Gestor da Internet exerce um grande papel consultivo e democrático na regulamentação e gestão da internet.

a governança da internet no Brasil, prevendo em seu item 6 que a filtragem ou privilégios de tráfego devem respeitar apenas critérios técnicos e éticos não sendo admissíveis motivos políticos, comerciais, religiosos, culturais ou qualquer forma de discriminação ou favorecimento²⁷.

Pela exposição acima, não resta dúvidas de que a discussão sobre neutralidade de rede se estabeleceu, inicialmente, adotando a internet como um meio de promoção aos direitos humanos e proteção do direito de escolha dos usuários.

Apesar da escolha humanística inicial, em um segundo momento, nos idos de 2011 em diante, os estudiosos, motivados pelas empresas de comunicação, se debruçaram no argumento mercadológico, almejando a implementação da neutralidade da rede com *granus salis*. Neste momento, o setor de provedores de acesso posicionou-se de forma bastante ativa durante o debate sobre neutralidade da rede no Brasil; em geral o setor se colocou a favor de uma regra de neutralidade da rede que vede expressamente o bloqueio de pacotes de dados, mas permita a discriminação por velocidade e preço²⁸.

O posicionamento era claro em buscar uma neutralidade relativa da rede, na medida em que se pudesse realizar uma gestão eficiente das redes e aumentasse o interesse em realizar investimentos. Para tanto, seria necessário que conferisse aos provedores de conexão a gestão autônoma do tráfego de suas redes com permissão de diferenciação de serviço e preço²⁹.

Fato interessante da época foi a Carta de Apoio ao Marco Civil da Internet

27. Disponível em <<https://www.cgi.br/media/docs/publicacoes/4/CGI-e-o-Marco-Civil.pdf>>. Acesso em 01/07/2024 às 11:39hs.

28. RAMOS, Pedro Henrique Soares. *Arquitetura da rede e regulação: a neutralidade da rede no Brasil*. Dissertação (Mestrado em Direito) - FGV - Fundação Getúlio Vargas, São Paulo, 2015, pág. 72)

29. “Uma posição divergente no setor foi emitida pela Associação Brasileira de Provedores de Internet e Telecomunicações (Abrint), entidade que representa pequenos provedores regionais que, em nota publicada em setembro de 2012, defendeu a aprovação de uma regra de neutralidade da rede no Marco Civil, ressaltando que “a população não pode ficar a mercê dos interesses comerciais dos grandes operadores de telecomunicação que, em um ambiente sem neutralidade, poderiam determinar conteúdos que fossem adequados aos seus negócios e interesses”. (RAMOS, Pedro Henrique Soares. *Arquitetura da rede e regulação: a neutralidade da rede no Brasil*. Dissertação (Mestrado em Direito) - FGV - Fundação Getúlio Vargas, São Paulo, 2015. Pág. 73/74)

elaborada pelo Google, Facebook (atual Meta) e Mercado Livre no sentido de apoiar o projeto de lei que resultou na publicação do Marco Civil da Internet. Apesar de não terem defendido expressamente a neutralidade da rede, concordaram com a proteção dos direitos arrolados no projeto, em especial a inviolabilidade e sigilo das comunicações e a não suspensão da conexão à internet, bem como anuíram com a função social dos provedores de serviços da internet, como catalizadores de interações sociais e “potencial democratizante da Internet”³⁰

Não obstante o intenso debate, o Marco Civil da Internet, acabou por adotar o caráter protetivo e em seu artigo 9º positivou o conceito de neutralidade de rede como dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação.

O legislador optou por uma ideia proativa de atuação dos provedores de acesso porquanto se utilizou a expressão de tratamento isonômico e não omissiva de “não discriminação. A escolha traz uma salutar obrigação positiva e não apenas negativa, em estrita consonância ao um novo paradigma dogmático de *compliance* e boas práticas empresariais.

Optou-se também por buscar abarcar a todos aqueles sujeitos que tratam do roteamento, comutação e transmissão de pacotes de dados, não se limitando apenas aos responsáveis pela transmissão final dos pacotes. Em relação ao objeto, o conceito não faz qualquer discriminação, cabendo o entendimento de que a neutralidade de rede se aplica a todos e quaisquer pacotes de dados.

A amplitude conceitual, portanto, não confere um caráter absoluto à neutralidade de rede, cuja interpretação deve ser realizada sempre em consonância com os fundamentos, princípios e objetivos correlatos a boa governança da internet. Por força desse ecossistema dogmático, admite-se a realização de discriminações no tráfego de dados a priorização de determinados pacotes em face de outros, o que teceremos breves comentários.

A análise do alcance do tratamento isonômico é de suma importância para que se tenha uma construção legítima da neutralidade de rede dentro de uma interpretação sistêmica do arcabouço principiológico do Marco Civil da Internet e demais

30. Disponível em <http://goo.gl/XC2rgu>. Acesso em 01/07/2024 às 17:29hs.

disposições correlatas.

2.3 Exceções à regra da neutralidade de rede

2.3.1 Hipóteses legais

A neutralidade de rede, assim como todos os direitos, não é absoluta e admite exceções em sua aplicação. Os parágrafos primeiro e segundo do artigo 9º do Marco Civil da Internet trouxeram as hipóteses legais, regulamentadas por ato privativo do Presidente da República, condicionados à oitiva do Comitê Gestor da Internet e Agência Nacional de Telecomunicações e desde que respeitadas algumas obrigações acessórias para a sua ocorrência.

A primeira hipótese de exceção consiste na discriminação ou degradação de tráfego em função de requisitos técnicos indispensáveis à prestação dos serviços e aplicações, cuja conceituação se divide em priorização de pacotes e segurança da rede³¹.

A priorização de pacotes decorre da própria estrutura do protocolo TCP/IP porquanto os pacotes de dados são identificados com informações suficientes para que haja a sua individualização pelos provedores de conexão³². Assim, é natural que haja

31. A questão de segurança na rede (cybersecurity) também tem sido alvo de diversos debates no campo de políticas públicas, e algumas das propostas interseccionam-se com a neutralidade da rede. Determinadas tecnologias, sites e aplicativos podem ser ameaças de segurança para usuários, empresas e governos, e bloqueios podem ser necessários para evitar a expansão dessas ameaças (Macdonald e Cannella, 2014). Governos e provedores de conexão precisam de um marco regulatório flexível para implementar inovações em suas redes que possam permitir o desenvolvimento de ferramentas mais modernas de segurança digital, como firewalls, software de segurança de rede, monitoramento de infraestruturas e bloqueios automáticos de ameaças (Crews, 2013) (RAMOS, Pedro Henrique Soares. *Arquitetura da rede e regulação: a neutralidade da rede no Brasil*. Dissertação (Mestrado em Direito) - FGV - Fundação Getúlio Vargas, São Paulo, 2015. Pág. 113)

32. Por meio do protocolo TCP/IP, os pacotes de dados transmitidos através da rede (payloads) são individualmente empacotados e identificados por meio de um cabeçalho de informações (IP header), contendo os dados necessários para que provedores de conexão possam identificar como tratar o pacote de dados recebido. (...)Esse modelo estrutural do protocolo TCP/IP, com diversos hardware e software de gerenciamento de tráfego atualmente utilizados por provedores de conexão, busca endereçar, de forma dinâmica, uma das questões cruciais para a qualidade de experiência dos usuários: nem todos os pacotes de dados são iguais, e determinados pacotes são mais

uma priorização de determinados pacotes de dados em detrimento de outro, principalmente quando se tem um congestionamento da rede ou situações de latência, causas de sobrecarga da rede. Nestes casos, é legítima a atuação ativa do provedor de conexão em realizar uma gestão do tráfego, afim de priorizar determinados pacotes. Como exemplo clássico, tem-se a priorização de um conteúdo de vídeo transmitido por *streaming* em face de um e-mail.

Em igual importância se apresenta a segurança na rede, onde se permite certa vigilância dos dados transmitidos com vistas a monitorar determinados ataques e transmissão de dados que possam, ao menos potencialmente, gerar instabilidade na rede, interromper o funcionamento do sistema ou violar direitos dos usuários, para, enfim, bloqueá-los se confirmada a ameaça ou lesão.

A segunda hipótese permissiva de discriminação corresponde à priorização de pacotes para situações de emergência. A própria lei restringe a discriminação para priorizar as comunicações destinadas aos prestadores de serviços de emergência, comunicação entre eles ou comunicações necessárias para informar à população em situações de risco de desastre, de emergência ou de estado de calamidade pública³³.

sensíveis à latência que outros. Por exemplo, o atraso na entrega de um pacote de uma aplicação de VoIP ou de video streaming é muito mais prejudicial para a experiência do usuário do que o atraso na entrega de um e-mail. Além disso, determinados dados consomem muito mais recursos de rede do que outros, e provedores de conexão precisam também endereçar estratégias de priorização de tráfego que permitam a gestão eficiente de seus recursos.” RAMOS, Pedro Henrique Soares. *Arquitetura da rede e regulação: a neutralidade da rede no Brasil*. Dissertação (Mestrado em Direito) - FGV - Fundação Getúlio Vargas, São Paulo, 2015. Pág. 109

33. Nos EUA, o FCC mantém um programa denominado *Telecommunications Service Priority (TSP)*, que obriga provedores de acesso a fornecerem tratamento prioritário a serviços que sejam considerados de emergência e de interesse nacional crítico, em caso de calamidades como desastres naturais e outras situações em que há potencial risco às vidas e propriedade de cidadãos estadunidenses. No Brasil, o Regulamento da SCM da Anatel estabelece, em seus artigos. 59 a 61, que os provedores de acesso devem “atender com prioridade o Presidente da República, seus representantes protocolares, sua comitiva e pessoal de apoio, bem como os Chefes de Estado estrangeiros, quando em visitas ou deslocamentos oficiais pelos território brasileiro, tornando disponíveis os meios necessários para a adequada comunicação dessas autoridades”, bem como “colocar à disposição das autoridades e dos agentes da defesa civil, nos casos de calamidade pública, todos os meios, sistemas e disponibilidades que lhe forem solicitados com vista a dar-lhes suporte ou amparar populações atingidas, na forma da regulamentação.” RAMOS, Pedro Henrique Soares.

Tamanha é a sensibilidade da questão – por vezes influenciada por questões políticas – que a lei e o decreto regulamentador trouxeram importantes limites aos provedores de acesso no exercício da sua gestão do tráfego discriminatória legalmente permitida, reduzindo a sua discricionariedade a patamares mínimos de atuação.

Em caráter macro sistêmico somente se permite o gerenciamento de rede pelos provedores de acesso com o objetivo de preservação da estabilidade, segurança e funcionalidade da rede, mediante a utilização de medidas técnicas compatíveis com padrões internacionais, e observados parâmetros regulatórios expedidos pela Anatel³⁴ e as diretrizes do CGI.br, proporcionalmente realizadas, abstendo-se, sempre que possível, de causar danos aos usuários³⁵.

Em âmbito individualmente considerado, exige-se a adoção de medidas de transparência em face dos usuários, em medida que se consiga explicitar o motivo do gerenciamento que implique a discriminação ou degradação, todos com linguagem compreensível e contendo, no mínimo, descrição das práticas, efeitos da sua adoção e os motivos e necessidade da adoção destas práticas, manifestadas em indicação contratual da medida e divulgação no site,³⁶.

A regulamentação ainda veda expressamente condutas unilaterais ou acordos entre os provedores de conexão e os provedores de aplicação que comprometam o caráter público e irrestrito do acesso à internet, fundamentos, princípio ou objetivo; priorizem pacotes de dados em arranjos comerciais e privilegiem aplicações próprias ou de parceiros comerciais³⁷.

Conclui-se que a exceção à neutralidade de rede vem carregada de propósitos bem definidos e eminentemente direcionados à proteção do sistema, sua estabilidade, segurança e funcionalidade, condicionados ainda ao dever de prestar informações prévias e claras aos usuários em medidas proporcionais e sem causar danos. Caso haja

Arquitetura da rede e regulação: a neutralidade da rede no Brasil. Dissertação (Mestrado em Direito) - FGV - Fundação Getúlio Vargas, São Paulo, 2015. Pág. 118/119

34. Atualmente, as Resoluções n. 739 e 740 de 2020, regulamentam o uso e serviços de telecomunicações em desastres, situações de emergência e calamidade; e segurança cibernética, respectivamente.

35. Art. 9º, § 2º da Lei 12.965/14

36. Artigos 6º e 7º do Decreto 8.771, de 11 de maio de 2016.

37. Artigo 9º do Decreto 8.771, de 11 de maio de 2016

cumprimento de todas as obrigações e respeito aos limites acima as discriminações perpetradas serão legais e, mais do que isso, legítimas.

Logicamente esse cenário límpido não se sustenta em um contexto de participação com vários atores com interesses conflitantes dentro de uma internet dinâmica e com uma fluidez peculiar. Em vários momentos algumas práticas mercadológicas foram objeto de grandes reflexões e desafios aos órgãos reguladores e fiscalizadores.

Nos próximos tópicos analisaremos alguns dos mais relevantes.

2.3.2 Zero Rating

O *zero rating* se perfaz em uma prática de mercado onde o provedor de acesso não contabiliza o uso dos dados de uso de determinados provedores de aplicação, em função de um acordo comercial. Isso significa que o usuário pode acessar o conteúdo com taxa zero sem contabilizar em sua quota geral de dados. A tarifa zero tende a ser uma característica dos mercados móveis, onde os pacotes de dados ilimitados não são tão universais como os de banda larga fixa³⁸.

Tal prática mercadológica se popularizou a partir de 2010 com o programa do *Facebook* (atual Meta) através do *Facebook Zero*³⁹, posteriormente com o *Twitter* (atual X), com o programa *Twitter Access*⁴⁰ e Google através do *Google Free Zone*⁴¹.

Em que pese a difusão mundial da prática mercadológica, a discussão sobre os benefícios e prejuízos aos usuários e à neutralidade de rede trazidos pelo *zero rating*

38. Tradução livre: “This means that the customer can access the zero-rated content without it counting towards their general data allowance. Zero-rating tends to be a feature of mobile markets, where unlimited data packages are not as universal as for fixed broadband”. (Ofcom; Reino Unido, 2024; < <https://www.ofcom.org.uk/internet-based-services/network-neutrality/net-neutrality-review/>>. Acesso em 17/06/2024, pág. 37)

39. Disponível https://m.facebook.com/nt/screen/?params=%7B%22note_id%22%3A270857300920606%7D&path=%2Fnotes%2Fnote%2F. Acesso em 02.07.24 às 11:37hs

40. Disponível https://en.wikipedia.org/wiki/Twitter_Zero#:~:text=Twitter%20Zero%20is%20an%20initiative,only%20version%20of%20the%20website.>. Acesso em 02.07.24 às 11:41hs

41. Disponível <https://googlesystem.blogspot.com/2012/10/google-free-zone.html>. Acesso em 02.07.24 às 11:44hs.

se manteve e se mantém intensa, com satisfatórios argumentos apresentados por ambos os lados.

Em defesa à prática do *zero rating* argumenta-se que a sua implementação é um benefício a ser oferecido aos usuários, mediante a preservação do seu pacote de dados no acesso de determinados aplicativos. Corolário deste argumento tem-se a defesa de uma redução dos custos de acesso à internet e a possibilidade de acesso gratuito a conteúdos educativos com a promoção da democratização da internet⁴². Os defensores ainda se debruçam na liberdade econômica, livre iniciativa e a liberdade dos modelos de negócios, cujos princípios estão protegidos pela Constituição Federal⁴³ e replicados no Marco Civil da Internet⁴⁴.

Em sentido oposto, os críticos do *zero rating* entendem que a prática mercadológica detém capacidade de reduzir o direito de escolha dos usuários, tendo em vista a disponibilidade de acesso gratuito a poucas aplicações. Argumenta-se ainda a possibilidade de influências políticas dos governos sobre seus cidadãos, principalmente em países autoritários, além da criação de uma barreira entre os usuários com maior

42. Na medida em que grandes provedores de conteúdo precisam aumentar suas bases de dados para a oferta de serviços de publicidade, é natural que essas empresas busquem uma atuação mais forte em grandes mercados consumidores localizados em países em desenvolvimento. Todavia, quando essas empresas iniciam suas operações nesses países, estas se veem em condições econômicas adversas para o desenvolvimento de operações locais, tendo em vista que a penetração da internet é baixa, os custos de acesso são ainda altos e celulares ainda são a principal porta de entrada para a internet. Uma das formas que provedores de aplicação encontram para desenvolver suas operações locais e, ao mesmo tempo, o desenvolvimento do ecossistema local, são parcerias como *zero-rating*, oferecendo assim planos de acesso patrocinado a usuários de operadoras locais. (RAMOS, Pedro Henrique Soares. *Arquitetura da rede e regulação: a neutralidade da rede no Brasil*. Dissertação (Mestrado em Direito) - FGV - Fundação Getúlio Vargas, São Paulo, 2015, pág. 161)

43. Art. 170 A ordem econômica, fundada na valorização do trabalho humano e na livre iniciativa, tem por fim assegurar a todos existência digna, conforme os ditames da justiça social, observados os seguintes princípios: I - soberania nacional; II - propriedade privada; III - função social da propriedade; IV - livre concorrência; V - defesa do consumidor; VI - defesa do meio ambiente, inclusive mediante tratamento diferenciado conforme o impacto ambiental dos produtos e serviços e de seus processos de elaboração e prestação; VII - redução das desigualdades regionais e sociais; VIII - busca do pleno emprego; IX - tratamento favorecido para as empresas de pequeno porte constituídas sob as leis brasileiras e que tenham sua sede e administração no País.”

44. Artigo 2º, V e artigo 3º VIII

capacidade financeira e os menos afortunados, criando-se mais uma forma de exclusão social pela divisão explícita entre uma “internet dos ricos” e uma “internet dos pobres. No âmbito concorrencial haveria um aprofundamento do monopólio das *bigtechs* e o aumento das barreiras à entrada de novos *players* e do aumento dos incentivos à inovação⁴⁵.

O CADE frente a esse impasse foi provocado pelo Ministério Público Federal (“MPF”) sobre a prática do *zero rating* praticado pelas principais operadoras de telefonia móvel, o que resultou na abertura de um Inquérito Administrativo para apuração de infrações à ordem econômica⁴⁶.

Segundo a denúncia do MPF, as operadoras de telefonia celular, controladoras de quase a totalidade do mercado, estariam adotando práticas comerciais discriminatórias no provimento do serviço de acesso à Internet móvel, ao ofertar a seus usuários planos de dados que diferenciam as condições de acesso a determinados serviços de Internet, por meio da cobrança de valores reduzidos ou mesmo da isenção total de cobrança.

As operadoras de telefonia celular, em defesa, apresentaram argumentos meritórios diversos.

A VIVO S/A afirmou que não pratica o *zero rating* em todos os modelos que adota atualmente e que suas políticas comerciais possuem justificativas legítimas e seriam uma estratégia lícita de diferenciação tanto por parte da empresa quanto por parte

45. “Nesse cenário, as aplicações de maior sucesso não serão necessariamente aquelas que possuem a melhor tecnologia e desenvolvem o melhor produto, mas sim as aplicações que conseguirem a melhor condição de acesso junto a provedores de acesso²⁹⁴. Destarte, se determinada startup resolve competir em um setor em que já existe um concorrente que possui um acordo de zero-rating com um provedor de acesso, essa startup deverá enfrentar a barreira de que, pela perspectiva do usuário, a aplicação oferecida por esta é paga, enquanto a do concorrente é gratuita.” RAMOS, Pedro Henrique Soares. *Arquitetura da rede e regulação: a neutralidade da rede no Brasil*. Dissertação (Mestrado em Direito) - FGV - Fundação Getúlio Vargas, São Paulo, 2015, pág. 160

46. Inquérito Administrativo n. 08700.004314/2016-71. Disponível em https://sei.cade.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?DZ2uWeaYicbuRZEFhBt-n3BfPLlu9u7akQAh8mpB9yOTVltdzdZLqhkfL-gLcg20sp2COFkT0u4F6kpO2C8HmeI4kRnRnEVbwvcVZhI5-Ryodazm-kfXdvuF-MMocM8XW

dos próprios sites e aplicativos, e estimulariam a concorrência.

A TIM S/A defendeu a licitude do modelo de negócio baseado em *zero rating* frente ao Marco Civil da Internet e que a oferta “Tim Controle WhatsApp” evidência, não somente, a inexistência de potenciais efeitos anticompetitivos, como também a existência de eficiências significativas.

Segundo a CLARO S/A, as políticas comerciais e promoções implementadas pela operadora não possuem o objeto e nem poderiam produzir qualquer efeito anticompetitivo e, dessa forma, não configuram infração à ordem econômica prevista na Lei nº 12.529/2011. Destacou ao contrário, suas promoções de *zero rating* teriam o potencial de gerar uma série de efeitos benéficos e pró-competitivos no mercado, que foram desconsiderados na Representação do MPF.

A Oi Móvel S/A sustentou que suas ofertas são perfeitamente lícitas, uma vez que que não há produção de efeitos anticompetitivos nos mercados de telefonia móvel ou de aplicações de Internet. Concluiu que tanto o *zero rating* quanto o acesso patrocinado são claramente benéficos à competição, gerando incentivos à inovação e possibilitando uma maior disputa pelo consumidor

A Anatel se manifestou pela ausência de indícios de infração da ordem econômica nas ofertas dos planos contendo cláusulas *zero rating* das prestadoras do Serviço Móvel Pessoal, encaminhando, por conseguinte, a íntegra dos autos do Processo n. 53500.020772/2016-69. Em síntese, a análise empreendida pela Agência no referido processo, conclui que a conduta de *zero rating*, atualmente materializada nos planos de serviço das prestadoras do SMP representadas, não configuraria ameaça à livre concorrência, tampouco violaria o Marco Civil da Internet. A Anatel entendeu que, além de gerar ganhos de eficiência, a prática de preços diferenciados denunciada pelo MPF não produz efeitos limitadores da capacidade de inovação e do caráter disruptivo do mercado de provimento de conteúdo, e, por este motivo, não criaria barreiras à entrada no mesmo.

O CADE, em análise ao procedimento, sugeriu pelo arquivamento do Inquérito Administrativo ao entendimento de que não houve configuração de infrações das condutas apuradas, não havendo indícios de que as práticas denunciadas sejam capazes de gerar efeitos anticompetitivos. Ressalvou, no entanto, que o arquivamento não prejudica eventual investigação futura, diante da inexistência de novos indícios

de infração à ordem econômica a ensejar a continuidade da investigação.

Na sua decisão ainda destacou que o princípio da neutralidade não deve bloquear previamente ou desestimular os modelos de negócios das empresas da cadeia da internet, dentro de relações privadas, sendo admissível apenas o monitoramento e, quando for o caso, aplicar as medidas legais cabíveis⁴⁷.

A decisão acima conferiu fôlego às operadoras de telefonia móvel, mas não findou com a celeuma, mantendo-se a discussão viva e dotada de um aprofundamento fático-jurídico necessário.

Atualmente a tendência é de que a prática do *zero rating* seja analisada caso a caso a depender da origem da aplicação e do seu conteúdo. Em particular entende-se pela possibilidade de implementação do *zero rating* quando se trate de informações e serviços públicos do setor público e que proporcionem um benefício social; ou quando as ofertas de *zero rating* seja direcionada a uma classe de aplicações. Nesses casos entende-se, na verdade, que o *zero rating* é aconselhável e não apenas permitido.

Especificamente quanto ao *zero rating* ofertado pelas operadoras de telefonia móvel a discussão se esvaziou com a nova organização da Web 2.0, cenário em que as próprias operadoras já demonstram certo desinteresse pelo produto e tem, paulatinamente, reduzido a oferta em sua base de planos.

A celeuma agora se substitui pela possibilidade de se permitir uma contribuição das grandes geradoras de tráfego para financiamento das melhorias da infraestrutura de transmissão, afim de que se mantenha a qualidade da experiência do usuário e transmissão eficiente de dados, que será detalhada abaixo.

2.3.3 *Fair Share*

O *fair share* pode ser considerado como um compartilhamento justo dos custos correlacionados à atualização e manutenção da infraestrutura usada para viabilizar a

47. Para maior aprofundamento, sugere-se a leitura da Nota Técnica n. 34/2017/CGAA4/SGA1/SG/CADE. Disponível em https://sei.cade.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?DZ2uWeaYicbuRZEFhBt-n3BfPLlu9u7akQA8mpB9yOTVltdzdZLqhkflgLcg20sp2COFkT0u4F6kpO2C8HmeI4kRnR-nEVbwvcVZhI5-Ryodazm-kfXdvuF-MMocM8XW. Acesso em 02.07.24 às 15:14hs.

transmissão de dados. Em outras palavras, “Fair share”, ou “contribuição justa”, refere-se à proposta de repasse de parte dos custos de atualização e manutenção da infraestrutura que viabiliza o fluxo de dados digital às plataformas e grandes empresas de tecnologia produtoras de conteúdo⁴⁸.

O desenvolvimento dos provedores de aplicação, corolário do desestímulo à investimentos na infraestrutura herdada pelas empresas de telecomunicações, trouxe uma nova reorganização do ecossistema da internet, onde os provedores de aplicação demandam parcela significativa do tráfego de dados.

Segundo o levantamento realizado pela Anatel na Tomada de Subsídios n. 13/2023⁴⁹ e, posteriormente, na Tomada de Subsídios n. 26/2024⁵⁰, o tráfego em 2023 chegou a ultrapassar 26,3 terabites nos pontos de troca, sendo as principais redes sociais (*Facebook, Instagram e X*) responsável por praticamente 50% do tráfego gerado nas redes. Nas redes móveis, o *streaming* de vídeo e redes sociais correspondem à 82,5% do tráfego total. Há uma alta concentração de relevante percentual do tráfego de dados a poucos *players*, eminentemente as *big tech*⁵¹.

Este novo cenário trouxe uma assimetria entre as empresas de telecomunicações e as empresas de tecnologia (*provedores de aplicação*), com possibilidade de comprometimento da acessibilidade digital e sustentabilidade dos custos da infraestrutura digital.

Em que pese o entendimento de que a construção de uma internet harmoniosa, plural e integra depende de todos os envolvidos em sua utilização, o custeio da manutenção e atualização de toda infraestrutura de telecomunicações recai sobre as empresas de telecomunicações. Aqui, vale relembrar que o serviço de internet não é um

48. FREIRE, Alexandre; CAMPOS, Ricardo. *Fair Share: entre infraestrutura digital e fluxo de serviços e dados*. Disponível em < <https://www.jota.info/opiniao-e-analise/artigos/fair-share-entre-infraestrutura-digital-e-fluxo-de-servicos-e-dados-24012023>>. Acesso em 02/07/2024 às 16:42hs

49. Disponível em < <https://apps.anatel.gov.br/ParticipaAnatel/VisualizarTextoConsulta.aspx?TelaDeOrigem=2&ConsultaId=10120>> Acesso em 03/07/2024 às 09:34hs

50. Disponível em <https://apps.anatel.gov.br/ParticipaAnatel/VisualizarTextoConsulta.aspx?TelaDeOrigem=2&ConsultaId=20202>. Acesso em 03/07/2024 às 09:35hs

51. Os aplicativos de Netflix, Youtube, Disney+, TikTok e Amazon Prime tem 37,8% do tráfego *downstream* segundo Relatório “Global Internet Phenomena Report” da Sandvine. Vídeos em geral representam 65,93% do tráfego nas redes.

serviço de telecomunicações propriamente dito, mas ainda é considerado um serviço de valor adicionado, conceituado como atividade que acrescenta, a um serviço de telecomunicações que lhe dá suporte e com o qual não se confunde, novas utilidades relacionadas ao acesso, armazenamento, apresentação, movimentação ou recuperação de informações⁵².

A Conexis Brasil Digital, em levantamento realizado para carrear a Tomada de Subsídios n. 13/2023 apurou que o investimento realizado pelas empresas de telecomunicações, em 2021, atingiu, aproximadamente, R\$ 102,5 Bilhões, sendo tal valor direcionado à investimentos de infraestrutura, aquisição de espectro, expansão e automação de *Content Delivery Networks* (“CND”), investimentos em rede de acesso e transmissão, incluindo conectividade satelital, *off-load* das redes móveis por WiFi apoiadas em redes *Fiber-to-the-home* (FTTH), novos *sites* e *datacenters*, e os recursos necessários em transmissão de dados para a integração destes centros⁵³.

Os provedores de aplicação, representadas pelas *Big Techs*, por sua vez, se aproveitam desse ecossistema sem, contudo, contribuir adequadamente⁵⁴ na manutenção e atualização da infraestrutura que usufrui frente a lucros exorbitantes que aferem em seus modelos de negócio.

Essa falha de mercado suscitou a discussão sobre a criação de uma contribuição

52. “Art. 61 da Lei 9.472/97 – Lei Geral de Telecomunicações

53. Informação extraída do item 1.1.2 – Uso de redes de telecomunicações no tráfego de dados para suporte aos serviços de valor adicionado e no tráfego de voz de modo massivo, da Tomada de Subsídio n. 26/2024.

54. Apesar do entendimento de que os provedores de aplicação não contribuem adequadamente, restou comprovado na Tomada de Subsídios n. 13/2023 que as grandes plataformas digitais, indicaram na Tomada de Subsídios nº 13/2023, uma série de investimentos realizados por essas empresas em CDNs e *caches*, assim como cabos submarinos, gerenciamento do tráfego, serviços na nuvem, *data centers*, interconexão entre ISPs e *peering*, resiliência das redes, infraestrutura de redes de fibra óptica terrestre e redes satelitais, importando em benefícios para a melhoria da experiência do usuário, menor latência de rede, criação de demanda para as prestadoras e contribuição para eficiência de rede. Além disso, enfatizaram a melhoria da eficiência do uso da rede com a otimização de mecanismos de compressão de vídeo mais eficientes para mitigar o grande uso das redes por tráfego de vídeo. (Informação extraída do item 1.1.2 – Uso de redes de telecomunicações no tráfego de dados para suporte aos serviços de valor adicionado e no tráfego de voz de modo massivo, da Tomada de Subsídio n. 26/2024)

direcionada aos usuários da rede de transmissão, principalmente, por aqueles sujeitos que utilizam grande parcela do tráfego de dados, o que se denominou no *fair share*. Ultimamente essa discussão se tornou mais acirrada frente a perspectiva de um aumento exponencial da transmissão de dados, alimentado pela implementação da tecnologia 5G, difusão da Internet das Coisas e ampliação do acesso à internet⁵⁵.

Alguns países já se debruçaram sobre a questão. A Coreia do Sul aprovou, em 2020, a revisão do Telecommunications Business Act⁵⁶, apelidado de “Lei Netflix”⁵⁷, como uma tentativa de instar grandes operadoras estrangeiras a compartilhar custos para garantir serviços estáveis online. Nos Estados Unidos, o projeto de lei *Funding Affordable Internet with Reliable Contributions Act* ou *FAIR Contributions Act* (S. 2427) exige que a *Federal Communications Commission* (FCC) estude e relate a viabilidade de financiar o Fundo de Serviço Universal por meio de contribuições de provedores online de conteúdo e serviços.⁵⁸

O apoio institucional ao “fair share” também se reflete no Path to the Digital Decade da União Europeia. Trata-se de um programa político, adotado pelo Conselho — que representa os 27 governos da União Europeia — para tornar a Europa um líder tecnológico até 2030⁵⁹.

55. Segundo a pesquisa global do **DataReportal**, existem 5.36 bilhões de pessoas com acesso à internet, chegando a 66.2% da população mundial. Disponível < <https://v4company.com/blog/marketing-digital/digital-brasil-2024>>. Acesso em 03.07.24 às 10:10hs

56. Disponível em <https://thediplotmat.com/2021/08/netflix-and-sk-broadband-battle-over-who-pays-in-south-korea/>; Acesso em 03.07.24 às 10:15hs

57. “Na Coreia do Sul, o estrondoso sucesso da série “Round 6” fez com que o tráfego da Netflix explodisse 26 vezes na rede da SK Broadband, empresa de telecomunicações do país, causando dezenas de milhares de dólares em aumento de custos, o que levou a uma batalha judicial acerca do compartilhamento do ônus do custo de manutenção desse aumento. Após vitória da SKB na Corte Distrital do país, o caso segue em discussão em sede de recurso no Tribunal Superior de Seoul. (FREIRE, Alexandre; CAMPOS, Ricardo. *Fair Share: entre infraestrutura digital e fluxo de serviços e dados*. Disponível em < <https://www.jota.info/opiniao-e-analise/artigos/fair-share-entre-infraestrutura-digital-e-fluxo-de-servicos-e-dados-24012023>>. Acesso em 03/07/2024 às 10:18hs

58. Disponível em < <https://www.congress.gov/bill/117th-congress/senate-bill/2427>> Acesso em 03.07.24 às 10:19hs

59. FREIRE, Alexandre; CAMPOS, Ricardo. *Fair Share: entre infraestrutura digital e fluxo de serviços e dados*. Disponível em < <https://www.jota.info/opiniao-e-analise/artigos/fair-share-entre->

No Brasil a discussão ainda está em estágio preparatório de análise sobre o tema, através das tomadas de subsídios n. 13/2023 e 26/2024, concluída em 31/05/2024. Não obstante, já há uma movimentação legislativa com o projeto de lei 469/24 de autoria do Davi Soares, com contendo proibição expressa de que os provedores de conexão à internet instituem cobrança de tarifa para os provedores de conteúdo⁶⁰.

3. CONCLUSÃO

A neutralidade de rede se constituiu como um princípio vinculado à própria construção arquitetônica da internet, concebida primariamente como uma rede “*end-to-end*”, sem interferência do centro do sistema.

A evolução inicial da internet aliado à exigência da utilização da infraestrutura aproveitada para a prestação dos serviços de telecomunicações trouxe questionamentos quanto a liberdade econômica, direito de concorrência e iniciativa privada. Em reação ao movimento mercadológico, levantou-se a corrente humanista do uso da internet visando a proteção de direitos à liberdade de expressão, proteção à privacidade, acesso à educação, cultural, como um meio de participação democrática. Prevaleceu o entendimento protecionista da neutralidade da rede tendo no Brasil o Marco Civil da Internet como seu normativo principal e base jurídica para legislação em outros países.

Ultrapassado dez anos da publicação do Marco Civil da Internet o ecossistema da internet não é mais o mesmo. Os provedores de aplicação, outrora estimulados a ingressar em uma concorrência tecnológica, ocupam grande parcela do tráfego de dados e o acesso dos usuários, comprometendo a saúde da acessibilidade digital e sustentabilidade da infraestrutura.

Porquanto os provedores de aplicação auferem lucros e *valuation* empresarial cada vez mais exorbitantes, a responsabilidade pela manutenção e atualização da infraestrutura recai precipuamente sobre as empresas de telecomunicações, mesmo

infraestrutura-digital-e-fluxo-de-servicos-e-dados-24012023>. Acesso em 03/07/2024 às 10:18hs
60. Disponível em <https://www.camara.leg.br/noticias/1044591-proposta-proibe-provedor-de-internet-de-tarifar-plataformas-de-conteudo-por-uso-intensivo-da-rede>. Acesso em 03.07.24 às 10:29hs

sendo a internet um serviço de valor associado à telecomunicação. Este cenário com latentes falhas de mercado motivou a ocorrência de soluções empresariais destinadas a suprimir lacunas e manter o sistema oxigenado, como o *zero rating* e o *fair share*.

É inevitável que se revise a amplitude conceitual da neutralidade de rede ante o seu caráter multifacetário e complexo dos dias atuais, a fim de que se consiga atender equilibradamente os interesses de todos os envolvidos dentro deste novo cenário – e não aquele de 2014.

Nesta reavaliação os Estados terão um papel fundamental na construção paradigmática que melhor se adeque aos dias atuais e prepare um ambiente que não impeça a inovação e o avanço tecnológico, mas que mantenha um caráter protetivo dos direitos individuais e existenciais dos indivíduos dentro do mundo eletrônico, sob pena de uma implosão do ecossistema por seus próprios atores.

REFERÊNCIAS

- BELLI, Luca; DE FILIPPI, Primavera. *Net Neutrality Compendium: Human Rights, Free Competition and the Future of the Internet*. New York: Springer, 2016.
- BRASIL. Constituição da República Federativa do Brasil, de 10 de outubro de 1988. Governo Federal. <https://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc08.htm>.
- BRASIL. Norma 004/1995. *Uso de meios da rede pública de telecomunicações para acesso à internet*. Ministério Das Comunicações. < https://www.anatel.gov.br/Portal/verificaDocumentos/documento.asp?numeroPublicacao=10283&assuntoPublicacao=null&caminhoRel=null&filtro=1&documentoPath=biblioteca/Normas/Normas_MC/norma_004_95.htm>
- BRASIL. Lei 9.472, de 16 de julho de 1997. *Dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador e outros aspectos institucionais, nos termos da Emenda Constitucional n. 8, de 1995*. Governo Federal < https://www.planalto.gov.br/ccivil_03/leis/l9472.htm>
- BRASIL. Resolução n. 477, de 07 de agosto de 2013. *Aprova o Regulamento do Serviço Móvel Pessoal – SMP*. Agência Nacional de Telecomunicações. Disponível < <https://informacoes.anatel.gov.br/legislacao/resolucoes/2007/9-resolucao-477>>
- BRASIL. Resolução 614, de 28 de maio de 2013. *Aprova o Regulamento do Serviço de Comunicação Multímídia e altera os Anexos II e III do Regulamento de Cobrança de Preço Público pelo Direito de Exploração de Serviços de Telecomunicações e pelo Direito de Exploração de Satélite*. Agência Nacional de Telecomunicações Disponível < <https://informacoes.anatel.gov.br/legislacao/resolucoes/2013/465-resolucao-614>>.

BRASIL. Resolução n. 740 de 2020, de 21 de dezembro de 2020. *Aprova Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações*. Agência Nacional de Telecomunicações Disponível < <https://informacoes.anatel.gov.br/legislacao/resolucoes/2020/1497-resolucao-740>>

CNET. Estados Unidos, 2005. Disponível <<https://www.cnet.com/home/internet/telco-agrees-to-stop-blocking-voip-calls/>>

GETSCHKO, DEMI. *As origens do Marco da Internet*. In: Marco civil da Internet. Coordenadores: LEMOS, Ronaldo; LEITE, George Salomão Leite. Editora Atlas, São Paulo, 2014.

MARANHÃO, Juliano; MATTOS César. *Neutralidade de Rede VS Neutralidade Regulatória*. Legal Grounds Institute. São Paulo, 2024

PARENTONI, Leonardo. *Neutralidade da Rede: Mudanças na Infraestrutura da internet e como isso influencia na sua vida*. In: Revista Jurídica da Presidência. Janeiro de 2018. Disponível em <https://www.researchgate.net/publication/322838584_Neutralidade_de_rede_mudancas_na_infraestrutura_da_internet_e_como_isso_influencia_na_sua_vida>.

RAMOS, Pedro Henrique Soares. Arquitetura da rede e regulação: a neutralidade da rede no Brasil. Dissertação (Mestrado em Direito) - FGV - Fundação Getúlio Vargas, São Paulo, 2015.

170

Editora. Juiz de Fora, 2016.

WIKIPEDIA, Estados Unidos, 2024. Disponível https://en.wikipedia.org/wiki/Twitter_Zero#:~:text=Twitter%20Zero%20is%20an%20initiative,only%20version%20of%20the%20website.

WU, Tim. *Network neutrality, broadband discrimination*. J. on Telecomm. & High Tech. L., v. 2, 2003.

OS ASPECTOS ECONÔMICOS DO FAIR SHARE SOB A ÓTICA DA NEUTRALIDADE DA REDE

Fernanda Campos Botelho

Advogada e Mestra em Direito, Tecnologia e Inovação pela Universidade Federal de Minas Gerais. Advogada-sócia da Fernando Botelho Advogados. E-mail: fbotelho@fernandobotelhoadvogados.com.br

DOI: <https://doi.org/10.59224/dti7.ch5>

Resumo: Diante do aumento do consumo de *bytes* no ambiente *online* e da consequente necessidade de investimento na infraestrutura de transmissão na rede, o *fair share* surge como possível solução para o rateamento desse ônus suportado pelos provedores de conexão. É que, por meio desta prática, sugere-se o compartilhamento dos encargos com certos provedores de aplicação, que seriam os grandes consumidores de banda. Ocorre que tal prática, por se basear na discriminação de dados, acaba por esbarrar nas premissas do consagrado princípio da neutralidade de rede, grande legado do Marco Civil da Internet. Portanto, na comemoração dos 10 anos de vigência da referida lei, o presente artigo revisita essa discussão, com vistas a traçar previsões quanto ao tema no país.

Palavras-chave: *Fair share*; discriminação de dados; neutralidade de rede.

Abstract: *With the increase in online data consumption and the consequent necessity of high investment in net transmission, fair share emerges as a solution for the backbone providers to bear these new costs. On this regard, it is suggested that the excessive burdens are shared with some application providers, which are the major data consumers. However, the fact that this practice is based on data discrimination creates an important trigger that will threaten the legacy of the net neutrality principle. Thus, in the 10th anniversary of Civil Rights Framework for Internet in Brazil, this article will revisit this discussion, in order to predict the future of the subject.*

Keywords: *Fair share; data discrimination; net neutrality.*

SUMÁRIO: Introdução; 1. O *fair share*; 2. Os riscos à neutralidade de rede; 3. O caso *SK Broadband v. Netflix*; 4. O caso *Deutsche Telekom v. Meta*; 5. Os debates no Brasil quanto ao tópico; 6. Previsões e conclusões; Referências.

INTRODUÇÃO

A neutralidade de rede foi originalmente concebida pelo Professor da Universidade de Columbia Tim Wu (WU, 2003)¹ como um artifício para garantir aos usuários da rede mundial de computadores a liberdade de comunicação na internet.

O conceito, por sua vez, baseia-se na própria estrutura da internet, que foi idealizada como um ambiente construído colaborativamente por seus usuários, através do protocolo denominado *end-to-end*.

Nesse contexto, buscando manter a independência inerente ao meio, o princípio da neutralidade de rede se propõe a proteger a transferência de dados no ambiente *online*, garantindo que ela se dê de maneira indiscriminada pelos provedores de conexão.

Nas palavras de Wu, a internet deve ser vista pelos desenvolvedores de aplicações como um ambiente competitivo, onde se disputa a atenção do usuário. Logo, a neutralidade do meio é imprescindível para manter a meritocracia da competição².

Dessa forma, o princípio garante a todos os usuários a liberdade no uso da rede, assegurando-lhes, com isso, que os dados enviados ou recebidos sejam tratados e processados no ambiente *online* de maneira uniforme, sem qualquer discriminação em virtude de sua origem, destino, tamanho, formato ou conteúdo.

Pois bem.

Por mais que a neutralidade de rede seja inerente à arquitetura e ao funcionamento da internet, em se tratando do Brasil, foi somente em 23 de abril de 2014, quando sancionado o Marco Civil da Internet (Lei n. 12.965/2014), que esta se tornou um princípio positivado.

1. WU, Tim. *Network Neutrality, Broadband Discrimination*, 2 J. on Telecomm. & High Tech. L. 141, 2003.

2. “A communications network like the Internet can be seen as a platform for a competition among application developers. Email, the web, and streaming applications are in a battle for the attention and interest of end-users. It is therefore important that the platform be neutral to ensure the competition remains meritocratic”. WU, Tim. *Network Neutrality, Broadband Discrimination*, 2 J. on Telecomm. & High Tech. L. 141, 2003

Aliás, em momento imediatamente anterior à aprovação do projeto de lei que originou o Marco Civil da Internet, a neutralidade de rede ali disciplinada foi objeto de extensas discussões e acarretou em consecutivos adiamentos na votação do texto na Câmara dos Deputados.

Logo, foi em meio a polêmicas, discordâncias e conflitos de interesses que a neutralidade de rede restou positivada, no artigo 3º, inciso IV do diploma, como princípio que norteia o uso da internet no país.

Não obstante, em virtude da relevância da matéria e da complexidade dos debates, o temário ganhou, também, seção própria dentro do capítulo 3 da lei, onde restou conceituado e balizado.

Assim, sob o artigo 9º do diploma legal, que inaugura este novo capítulo, ficou preceituado o dever, por parte do responsável pela transmissão, comutação ou roteamento de dados, do tratamento isonômico dos pacotes, sem que seja feita distinção em virtude do conteúdo, origem, destino, serviço, terminal ou aplicação.

Ainda, restaram disciplinados, nos parágrafos 2º e 3º da norma, respectivamente, as exceções legais permissivas da discriminação de dados e a proibição do bloqueio, filtro, monitoramento ou análise dos pacotes de dados por parte dos provedores de serviços na internet.

Com isso, às empresas de telecomunicações restou limitada³ a possibilidade anteriormente praticada da venda de pacotes de dados com limitações de acesso, bem como restou assegurada a competitividade entre os provedores de aplicação.

Atualmente, completados 10 anos de vigência do Marco Civil da Internet, o princípio da neutralidade de rede toma modernos e diferentes contornos, tendo de se reafirmar numa realidade comandada pelo aumento intenso do fluxo, da velocidade e do consumo de dados.

Isso porque os provedores de conexão, diante da total preponderância do

3. Já que tida pelo Conselho Administrativo da Defesa Econômica (CADE) como não contrária à lei e à ordem econômica a prática do *zero rating*. (CADE, 2017). *NOTA TÉCNICA Nº 34/2017/CGAA4/SGA1/SG/CADE*. Disponível em: https://sei.cade.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?DZ2uWeaYicbuRZEFhBt-n3BfPLlu9u7akQA8mpB9yOTVltdzdZLqhkflgLcg20sp2COFkT0u4F6kpO2C8HmeI4kRnR-nEVbwvcVZhI5-Ryodazm-kfXdvuF-MMocM8XW%3E

ambiente de rede sobre os demais⁴ e do aumento não só do consumo de *bytes*, mas da demanda por velocidade de conexão, têm de aumentar os investimentos em infraestrutura de rede, sob pena de não conseguir prestar o serviço proposto.

É, portanto, na era da *Big Data*, onde a rede mundial de computadores restou dominada pelas *Big Techs*, que emergirá o *fair share* como possível solução econômica para que a infraestrutura de rede acompanhe o novo padrão de consumo de dados.

No entanto, por mais que elencado como solução aos novos modelos de negócio, este chamado “pedágio na internet” acaba por esbarrar nos pilares da aclamada neutralidade de rede, o que leva a questionamentos quanto a sua legalidade e quanto à necessidade de fixação de critérios e parâmetros para seu estabelecimento.

1 O FAIR SHARE

O *fair share* - termo cuja tradução seria “contribuição justa” - diz respeito à proposta criada, em meados da década de 90, pelo operadores de internet europeus pertencentes a organizações como a *European Telecommunications Network Operators* e a *Global System for Mobile Communications Association*.

Tratou-se, em suma, da proposição de compartilhamento dos custos de infraestrutura para transmissão de dados na rede entre os provedores de conexão e os provedores de aplicação, de modo que estes, sendo os maiores consumidores das bandas, arcariam com parte do investimento necessário à operação.

Assim, o mecanismo proposto pelos operadores de internet, que foi ali chamado de *Sending Party Network Pays*, obrigaria que a rede de onde se origina o envio dos dados pagasse uma taxa para a rede de destino.

A razão para tal proposta, no entanto, se vê no fato de que os grandes volumes de dados consumidos no mundo são fomentados pelo mesmo grupo de empresas de

4. De acordo com as estatísticas compartilhadas pelo IBGE, através do Módulo de Tecnologia de Informação e Comunicação (TIC) da PNAD Contínua, a internet era utilizada por 91,5% dos domicílios brasileiros no ano de 2022. Disponível em: <https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/38306-em-2022-streaming-estava-presente-em-43-4-dos-domicilios-com-tv> (IBGE, 2022)

tecnologia: as denominadas *Big Techs*.

Estas, por sua vez, demandam da rede mundial de computadores uma alta performance, de modo que os pacotes de dados produzidos e enviados cheguem aos usuários finais em curto espaço de tempo e com a qualidade almejada.

Ao mesmo tempo, estes usuários finais, que são, por lógica, os custeadores do serviço de rede utilizado, não tem como absorver os custos adicionais inerentes aos investimentos necessários para que a infraestrutura das conexões mantenha a qualidade da transmissão e do recebimento dos dados.

Dessa maneira, a lógica do *fair share* se operaria na possibilidade dos ditos grandes geradores de dados e grandes consumidores das bandas de conexão – conhecidos como *Over the Top* – remunerarem os provedores de acesso pela performance necessária nas redes para a transmissão de seus dados.

Por consequência, as operadoras de rede conseguiriam manter a entrega dos imensos volumes de dados, compartilhando, para isso, os custos de transmissão não só com os consumidores-usuários-finais, mas com as grandes plataformas.

Assim, acredita-se que, com o crescimento exponencial do volume de dados gerado na era do *Big Data*, o *fair share* seria a única alternativa para os provedores de conexão manterem a qualidade na entrega dos *bytes* aos usuários finais.

Propõe-se, então, que a contribuição voltada para a qualidade das conexões seja proporcional ao volume de dados gerado, de modo que quanto maior o consumo de rede e largura de banda, maior seria o chamado pedágio de uso da internet.

Neste contexto, a solução se apresenta sob diversas vertentes, podendo, inclusive, permitir que as empresas de telecomunicações estabeleçam distintas tratativas com as plataformas digitais, estabeleçam cobranças assimétricas ou, ainda, implementem a obrigatoriedade da contribuição para um fundo de conectividade.

Não obstante e para além dos apresentados benefícios da abordagem, aqueles que são favoráveis à proposta defendem que, em cenário contrário, ou seja, com a manutenção da divisão de custos da infraestrutura das conexões somente entre os operadores de rede e os consumidores finais, estaria comprometida, em poucos anos, a qualidade das conexões.

2 OS RISCOS À NEUTRALIDADE DE REDE

Apesar de ser evidente o crescimento exponencial do consumo de dados e a necessidade progressiva do aumento da qualidade das conexões, os críticos da proposta ainda veem no *fair share* muitos aspectos ameaçadores do que restou firmado por meio do princípio da neutralidade de rede.

Isso porque o princípio se baseia, como dito, na ideia da não discriminação entre os pacotes de dados, de modo que, independentemente de seu tamanho, volume, origem ou destino, estes devem ser tratados, pelos provedores de conexão, de maneira similar.

Assim, ao se estabelecer um custo maior de transmissão àqueles tidos como os maiores consumidores de banda, estar-se-ia atribuindo, aos *bytes* por eles gerados, um dispêndio maior, uma tratativa distinta, o que incorreria, justamente, na discriminação que o princípio da neutralidade de rede busca coibir.

De maneira ainda mais grave, tem-se que a prática do *fair share* tem o potencial de, inclusive, acarretar no bloqueio ou no limite de tráfego de serviços e, ao mesmo tempo, na priorização do curso de outros.

Assim, a cobrança de uma taxa extra às grandes plataformas poderia representar, para o consumidor final do serviço, uma redução na variedade e no volume dos dados consumidos, incorrendo, ainda, na restrição dos seus direitos previstos no Marco Civil da Internet.

Não suficiente, é de se elencar, também, o risco de que os provedores de rede estipulem dupla cobrança pelo mesmo serviço, uma vez que os usuários finais já arcam com os supostos custos de conexão oriundos de seus contratos com as empresas de telecomunicações, ao passo que estas, com a instituição do *fair share*, poderiam também cobrar, pelo mesmo múnus, dos provedores de aplicação.

3 O CASO SK BROADBAND V. NETFLIX

Apesar da temática do *fair share* estar em voga em todo o cenário internacional, tendo ocorrido, na União Europeia⁵, uma consulta pública sobre o futuro das

5. (UNIÃO EUROPEIA, 2023). Disponível em: <https://digital-178>

Os aspectos econômicos do *fair share* sob a ótica da neutralidade da rede telecomunicações e, nos Estados Unidos, a propositura de uma lei específica, o *Fair Contributions Act*⁶, foi na Coreia do Sul que a matéria tomou relevos significativos.

Isso decorre do fato de que um importante precedente judicial quanto ao tema se desenvolveu justamente no país, que é, por sua vez, internacionalmente reconhecido por sua alta capacidade relacionada à tecnologia da informação.

Neste contexto, tem-se que, no ano de 2018, a disputa judicial intitulada de *SK Broadband v. Netflix* se tornou uma espécie de *benchmarking* do tema.

O caso, por sua vez, consistiu em um litígio entre a gigante empresa de *streaming*, *Netflix*, e uma das mais renomadas provedoras de acesso à internet no país, que viria a ser, também, subsidiária da principal operadora de telefonia móvel – a *SK Telecom*.

A disputa se iniciou, como já dito, no ano de 2018, em um contexto em que o tráfego de dados aumentava exponencialmente no país, o que demandava das operadoras de serviço de internet uma modernização e um investimento relevante para a manutenção dos serviços de banda.

Assim, sob as descritas circunstâncias, a provedora de conexão *SK Broadband* solicitou, à *Netflix*, empresa que consumia volume de dados classificado como estratosférico, que custeasse as chamadas taxas de uso da rede, justamente em virtude do aumento de tráfego por ela gerado, que teria demandado alto investimento em infraestrutura para manter a qualidade e a alta definição prometidas ao usuário final dos dados produzidos e consumidos diretamente da plataforma de *streaming*.

No ano de 2020, no entanto, já em meio à pandemia do vírus COVID-19, o processo foi suspenso, em virtude de a plataforma *Netflix* ter buscado judicialmente a declaração de inexistência da obrigação de realizar pagamentos pelo uso da rede, com base, justamente, no princípio da neutralidade de rede, que impediria a discriminação e a cobrança diferenciada pelo tráfego de seus dados.

Porém, quando retomado o trâmite do feito, o Tribunal Distrital Central de Seul entendeu pela necessidade de fixação de uma compensação a ser prestada pela

strategy.ec.europa.eu/pt/consultations/future-electronic-communications-sector-and-its-infrastructure Acesso em: 01/06/2024

6. (EUA, Congresso, 2024). Congresso Norte-Americano. *Fair Contributions Act*. 2023-2024. Disponível em: <https://www.congress.gov/bill/118th-congress/senate-bill/856> Acesso em: 02/06/2024)

plataforma *Netflix*, em virtude de esta consumir um significativo volume de dados, onerando, para isso, imensa estrutura da operadora de rede.

A *Netflix*, por sua vez, recorreu da decisão para o Supremo Tribunal de Seul, que se propôs, em resposta, a elaborar parâmetros para a definição destas taxas de uso de rede, de modo que fossem considerados os custos totais da infraestrutura e o volume de tráfego produzido pelo provedor de conteúdo em questão.

Já em 2023, após intensas discussões judiciais e abordagens extrajudiciais, as empresas anunciaram a celebração de um acordo que poria fim ao litígio. Por meio deste, seria firmada, entre ambas, uma parceria estratégica para fornecer, aos usuários finais dos serviços, melhores condições por meio da aquisição de produtos combinados.

Com isso, apesar de não terem sido divulgados maiores detalhes do acordo firmado, entende-se que seria ofertada, aos consumidores, uma espécie de *cross-selling*, onde poderiam contratar os serviços de *streaming* da *Netflix* por meio de sua assinatura de banda larga, de modo que os custos do intenso tráfego de dados estariam acobertados nesta proposta comercial.

Logo, verifica-se que, para por fim à disputa, os provedores se uniram de modo a deslocar os encargos em discussão para o consumidor final, por meio da oferta de proposta conjunta das empresas em destaque.

A importância do precedente, contudo, não se resume ao pioneirismo do debate e nem aos mais diversos dados estatísticos trazidos aos autos, mas abrange a solução dada ao caso concreto.

É que, como visto, o acordo e a tratativa realizados somente entre os provedores de serviço desperta atenção para o risco gerado ao consumidor diante da ausência de regulamentação do tema.

Não suficiente e de maneira ainda mais relevante, o caso enriquece a discussão quanto aos possíveis modelos de negócio a serem firmados pelos *players* envolvidos no debate, o que atribui valor econômico à pauta e torna imprescindível a participação ativa da sociedade civil na construção da solução a ser aplicada nos mais diversos cenários.

4 O CASO DEUTSCHE TELEKOM V. META

Mais recentemente, após a resolução do caso envolvendo a *Netflix* e durante a pandemia do vírus COVID-19, outro litígio versando sobre a prática do *fairshare* inaugurou debates acerca do tema na Alemanha.

Tratou-se, por sua vez, de processo envolvendo a *big tech Meta* e a operadora de serviços de telecomunicações *Deutsche Telekom*, no qual esta acusou aquela de promover, unilateralmente, a rescisão de contrato de transporte de dados celebrado entre ambas há dez anos e continuar a usar a infraestrutura de rede de maneira gratuita.

Ocorre que, como afirmado pelo vice-presidente da operadora, *Wolfgang Kopf*, as empresas celebraram, no ano de 2010, um acordo por meio do qual a *Meta* pagava, à provedora de rede, uma taxa de aproximadamente 5,8 milhões de euros por ano pelo serviço de transporte de dados. Assim, após pleitear, sem sucesso, a redução drástica da referenciada taxa, *Meta* optou pela rescisão do vínculo.

No entanto, mesmo após a dita rescisão, a empresa teria continuado a enviar, por meio da conexão fornecida pela operadora, consideráveis volumes de dados, entendendo, assim, possuir o direito de uso gratuito da conexão de rede.

Com isso, no mês de julho do ano de 2021, a operadora de serviços de rede entrou com uma ação judicial contra a subsidiária alemã da *Meta*, onde pleiteou a interrupção do uso ou o restabelecimento do contrato e do pagamento.

Já no âmbito da ação judicial, a ré defendeu que a cobrança da taxa de transmissão de dados era ilegítima, se enquadrando como prática de abuso de poder de mercado, motivo pelo qual deveria ser suprimida.

Apesar disso, o Tribunal Regional de Colônia, na Alemanha, julgou procedente a ação para condenar a empresa de mídia social a pagar aproximadamente 20 milhões de euros à provedora de serviços de telecomunicações, em virtude de, mesmo após ter interrompido o vínculo contratual, ter mantido a utilização do serviço de transporte de dados, o que incorreria no consentimento da manutenção do vínculo.

Assim, transcendendo à solução individual dada ao processo *sub judice*, a importância do precedente diz respeito ao fato de este tratar da legitimação do *fair share*, uma vez que a validação da cobrança de taxa por serviço de transporte de dados acaba por assentir com a possibilidade da imposição do encargo por todas as demais

empresas do ramo das telecomunicações no país e até no continente europeu.

Sob esta exata perspectiva, no mês de maio do ano de 2024, a referida Corte confirmou a legitimidade do *fair share*, porém acabou deixando em aberto a discussão quanto à quantificação do encargo a ser estabelecido pelo uso do serviço de transporte de dados.

Dessa forma, mostrou-se relevante, especialmente *in casu*, que seja ainda estabelecida uma regulação para a quantificação desses encargos de maneira apropriada, o que impediria o acionamento massivo do judiciário para resolução de disputas relativas a tarifas estabelecidas em *fair share*.

5 OS DEBATES NO BRASIL QUANTO AO TÓPICO

No mês de março de 2023, a Anatel⁷ abriu a Tomada de Subsídios n. 13/2023, que dizia respeito à regulamentação⁸ dos deveres dos usuários dos serviços de telecomunicações e, em específico, buscava informações sobre a necessidade de fixação de regras próprias para os chamados grandes usuários, que seriam justamente aqueles classificados como de alto valor agregado e definidos no art. 61 da Lei Geral de Telecomunicações (Lei n. 9.472/ 1997)⁹.

Nesse sentido, é importante ressaltar que a referida Tomada de Subsídio se prestou ao estabelecimento de um canal de diálogo com os agentes interessados no objeto da consulta, justamente com o intuito de identificar problemas e reunir insumos para a elaboração da iniciativa regulamentar.

7. A Lei de Telecomunicações (Lei n. 9.472/1997) institui a Agência Nacional de Telecomunicações (ANATEL), bem como as prerrogativas necessárias ao exercício de sua competência.

8. Art. 19. À Agência compete adotar as medidas necessárias para o atendimento do interesse público e para o desenvolvimento das telecomunicações brasileiras, atuando com independência, imparcialidade, legalidade, impessoalidade e publicidade, e especialmente: (...)

X - expedir normas sobre prestação de serviços de telecomunicações no regime privado. (BRASIL, 1997)

9. Art. 61. Serviço de valor adicionado (SVA) é a atividade que acrescenta, a um serviço de telecomunicações que lhe dá suporte e com o qual não se confunde, novas utilidades relacionadas ao acesso, armazenamento, apresentação, movimentação ou recuperação de informações. (BRASIL, 1997)

Assim, por mais que a Anatel já possuísse regulação específica quanto aos deveres dos consumidores dos serviços de telecomunicações, a abertura visou debater, em especial, a necessidade de regras específicas para aqueles usuários que faziam uso massivo das redes de telecomunicações.

Com isso, pode-se dizer que a iniciativa consistiu em um primeiro passo, por parte da agência regulatória, para a regulamentação das plataformas digitais, bem como para o enquadramento destas como usuárias de fato dos serviços de telecomunicações.

Adentrando, todavia, a iniciativa propriamente dita, verifica-se que se deu de maneira *online* e contou com 28 perguntas a serem respondidas pelos contribuintes.

Essas perguntas, por sua vez, tratavam do modelo de negócios dessas plataformas digitais, de incentivos econômicos que poderiam ser gerados por parte do órgão regulador, de iniciativas de proteção aos direitos do consumidor, de iniciativas para a distinção, por parte dos consumidores, entre os serviços de telecomunicações e os serviços prestados pelos provedores de SVA, da construção de critérios para definição de diferentes categorias de usuário de serviços de telecomunicações, de medidas para a criação de modelos diferentes de remuneração de rede e para a garantia de que os recursos gerados sejam de fato investidos na infraestrutura das telecomunicações, da definição de prós e contras do estabelecimento de distintos modelos de remuneração de rede, seja pelo pagamento de *access fees* ou de *termination fees*, dentre outras¹⁰.

Para além disso, a iniciativa trouxe, como itens adicionais, relevantes informações e dados estatísticos colhidos, que serviriam, *in casu*, de embasamento e de contextualização para a coleta de informações.

Dessa forma, uma breve análise das mais importantes estatísticas apresentadas se mostra relevante para a contextualização da iniciativa, como se verá a seguir.

Primeiramente, merece destaque o tópico da pesquisa que enfatizou as evidências do uso massivo das redes de telecomunicações, com o aumento progressivo, desde o

10. (ANATEL, 2024). A íntegra das perguntas constantes da Tomada de Subsídios n. 13 pode ser consultada no sítio eletrônico da Anatel. Disponível em: <https://apps.anatel.gov.br/ParticipaAnatel/VisualizarTextoConsulta.aspx?TelaDeOrigem=3&ConsultaId=10120> Acesso em: 16/05/2024

ano de 2016, do tráfego de dados no país, o que sugeriria a existência de legitimidade da cogitação da prática do *fair share*.

Mas, de maneira ainda mais relevante, é de se mencionar que ficou ali demonstrado, pela *Pesquisa de Satisfação e Qualidade Percebida 2021* realizada pela Anatel, que o uso de aplicações como *streaming* de vídeo e redes sociais, que demandam maior volume de tráfego, é comum para a maioria dos usuários dos serviços de telecomunicações no Brasil.

Ademais, mostra-se de extrema relevância o fato de que ficou ali provado, por meio de dados fáticos, que o consumo de vídeo no ambiente *online* é relevante para 80% dos usuários de banda larga fixa. Assim, pode-se dizer que a maioria dos usuários atribui importância a conteúdos que correspondem, no tráfego *online*, a grandes e “pesados” volumes de dados, que acabam por onerar de forma significativa a rede.

De igual maneira, é digno de destaque, conforme ali demonstrado, o fato de que as redes sociais (*Facebook, Instagram, X*) são utilizadas constantemente por 85% dos usuários consumidores de banda larga fixa e 82% dos usuários do SMP Pós, de modo que pode ser constatado, pelo perfil de consumo representado na pesquisa referenciada, que grande percentual do tráfego total de dados está concentrado em poucos *players*: os grandes provedores de aplicação.

Ainda nesse sentido e exatamente quanto a estes grandes provedores de aplicação, são apresentados os seguintes dados: as plataformas *Netflix, Youtube, Disney+, TikTok, Amazon Prime* tem 37,8% do tráfego *downstream*, segundo o relatório *Global Internet Phenomena Report* da *Sandvine* e, quando analisados os dados, neste mesmo relatório, por grupo econômico, as denominadas *Big 6 (Meta, Alphabet, Microsoft, Amazon, Apple e Netflix)* representam quase 50% do tráfego de dados gerado na rede mundial de computadores.

Adentrando, então, às contribuições enviadas por aqueles que responderam à referida tomada de subsídios, pode-se afirmar a ocorrência de posicionamentos devidamente embasados em todos os sentidos: seja pela regulamentação de tratativa diferenciada aos chamados *heavy users*, que seriam os grandes consumidores das bandas de rede, seja pela desnecessidade de tratativa diferente entre os usuários dos serviços de telecomunicações.

No entanto, é de se destacar, dentre as ditas contribuições, a presença de diversas

entidades da sociedade civil, como a Internet Society (ISOC), o Instituto de Tecnologia e Sociedade do RJ (ITS), o Instituto de Referência em Internet e Sociedade (IRIS), o Instituto Brasileiro de Defesa do Consumidor (IDEC) e a Eletronic Frontier Foundation (EFF), que não somente elencaram a problemática relativa à competência da ANATEL para regulação da relação entre os provedores de conexão e os provedores de aplicação, mas, também, destacaram a fragilidade dos dados trazidos como embasamento da pesquisa, que poderiam, tal como proposto, contaminar a resposta objetiva aos questionamentos.

Com as conclusões obtidas da análise das contribuições recebidas, no mês de janeiro de 2024, e ainda sob a mesma lógica, a agência realizou nova Tomada de Subsídios (nº 26/2023)¹¹, agora com vistas à elaboração do chamado Regulamento de Deveres dos Usuários.

Nesta se buscava, de igual modo, o aprofundamento do debate quanto à necessidade de estabelecimento de regras específicas para os chamados grandes usuários que, enquadrados como provedores de Serviço de Valor Adicionado (SVA), por sua vez, demandariam um tratamento regulatório individualizado, em virtude de fazerem uso massivo das bandas de conexão.

Porém, de maneira distinta da primeira iniciativa, nesta a agência propôs, aos contribuintes, que respondessem específico questionamento quanto à existência de risco de desequilíbrio entre os prestadores de serviços de telecomunicações e provedores de SVA e quanto à possibilidade de ocorrência de reflexos na conectividade e no ecossistema digital.

Assim, elaborada de maneira diversa, esta segunda iniciativa contou com 6 temas abordados, com destaque especial ao *Tema 5*, que tratava dos investimentos que seriam cabíveis a cada agente do ecossistema digital em uma expansão da infraestrutura de rede.

Como resultado, verifica-se que foram recebidas 1.330 contribuições, além de 20 estudos técnicos fornecidos por operadoras de rede, organizações e integrantes da

11. (ANATEL, 2023). A íntegra da Tomada de Subsídios n. 26 pode ser consultada no sítio eletrônico da Anatel. Disponível em: <https://apps.anatel.gov.br/ParticipaAnatel/VisualizarTextoConsulta.aspx?TelaDeOrigem=2&ConsultaId=20202> Acesso em: 28/06/2024

sociedade civil.

Por meio destas respostas enviadas pelos mais diversos setores, buscou-se, então, a definição do termo *heavy users*, com o objetivo de enquadramento e estabelecimento de parâmetros para a categorização das organizações que usam as redes de forma massiva.

Pois bem.

Os debates acerca da temática do *fair share*, no entanto, não se restringiram a iniciativas da agência regulatória, de modo que, no dia 1º de novembro de 2023, a operadora de serviços de telecomunicações *TIM* promoveu um evento denominado *Diálogo Brasil-Europa sobre Agenda Digital e Fair Share*, que se propôs, justamente, a debater a universalização da conectividade.

O evento, que ocorreu de maneira presencial, na cidade do Rio de Janeiro, contou com a presença de representantes dos diversos atores interessados na temática: membros da Câmara dos Deputados, do Parlamento Europeu, diretores da Anatel, da GSMA, da Conexis, além de acadêmicos e executivos das principais operadoras de telefonia brasileiras.

Estes, por sua vez, defendendo as vertentes representativas do setor a que fazem parte, também se engajaram na discussão de mecanismos de equilíbrio e sustentabilidade financeira para os investimentos das companhias de telecomunicações, de modo a presumir como necessário o encargo para a manutenção da qualidade do tráfego de dados.

Independentemente das mencionadas discussões e tendo em vista, inclusive, o impacto econômico da eventual legitimação do *fair share*, a temática não poderia deixar de fazer parte da pauta legislativa, de modo que, desde o mês de fevereiro do ano de 2024, tramita, no Congresso Nacional, o Projeto de Lei 469/24, que busca, justamente, coibir a prática no Brasil, realizando, para tanto, um acréscimo no artigo 9º do Marco Civil da Internet.

Assim, objetiva-se, com a aprovação do projeto, a inserção, no Marco Civil da Internet, do artigo 9-A¹², que vedaria, aos provedores de conexão, a instituição de

12. (CÂMARA DOS DEPUTADOS, SÃO PAULO, 2024). Art. 9o-A. É vedada aos provedores de conexão de internet a instituição de cobrança por tráfego gerado por provedores de aplicações de

cobrança extra por tráfego gerado por provedores de aplicações, justamente em atenção e obediência ao princípio da neutralidade de rede.

A justificativa que ampara a referida proposta, no entanto, trata da essencialidade do serviço de conexão de rede e da tarifação do mesmo estar fundamentada na premissa de que os usuários finais devem contribuir financeiramente para o uso da conexão de acordo com o seu consumo de dados, o que asseguraria o balanceamento e a distribuição dos encargos, bem como a sustentabilidade financeira dos provedores de conexão de internet.

Ademais, o projeto defende que o estabelecimento do *fair share* entraria em conflito com o princípio da neutralidade de rede, por meio do estabelecimento de distinção entre os pacotes de dados com base no seu conteúdo, destino, origem ou volume.

Não suficiente, este defende, ainda, que a prática poderia afetar a livre concorrência e a inovação no ambiente *online*, uma vez que o volume de tráfego gerado serviria como pilar para o estabelecimento de tratativas discriminatórias entre os provedores de aplicação.

Ainda, este enfatiza existir um embate entre a prática do *fair share* e os preceitos do Código de Defesa do Consumidor (Lei n. 8.078, de 11 de setembro de 1990), já que ocorreria uma usurpação da definição do consumidor e os provedores de aplicação poderiam também se enquadrar no conceito.

Finalmente, este ressalta o risco da tarifação do tráfego de dados significar o repasse de custos extras aos consumidores finais, o que acarretaria no aumento do preço dos serviços fornecidos pelos provedores de aplicação sem uma simultânea redução nas tarifas firmadas pelos provedores de conexão e, assim, na dupla cobrança

internet, assegurada a manutenção dos princípios da neutralidade de rede previstos nesta Lei. Parágrafo único. A tarifação do uso da infraestrutura de rede dos provedores de conexão de internet serão aqueles estabelecidos nesta ou em outras Leis, devendo a regulamentação específica sobre tais temas se ater a questões procedimentais, respeitado o disposto no caput. (Projeto de Lei 469/24. Acrescenta o art. 90-A à Lei no 12.965, de 23 de abril de 2014 (Marco Civil da Internet), para proibir que provedores de conexão de internet instituem cobrança direcionada aos provedores de aplicações de internet por geração de tráfego de dados. Ano de 2024. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2390084&file-name=Tramitacao-PL%20469/2024. Acesso em: 15/06/2024)

pelo mesmo serviço.

Não obstante à iniciativa legislativa, é de se destacar que o posicionamento contrário ao estabelecimento do *fair share* também é disseminado pela grande maioria das associações representativas da sociedade civil, como a AbraCloud e a Abrint.

Neste contexto, merece realce o discurso trazido pela Associação que reúne a Cadeia Local de Nuvem no Brasil (AbraCloud), no sentido de que o estabelecimento de tarifas por meio da instituição do *fair share* pode ocasionar um retrocesso do ambiente *online*, com o conseguinte estabelecimento de barreiras à inclusão digital e à inovação.

Assim, de maneira oposta ao que pregam os defensores do *fair share*, os membros da associação argumentam que a crescente demanda por conexão e aumento de banda decorrente do crescimento do consumo de dados estaria solucionada, automaticamente, por meio da verba gerada com as novas vendas de planos de Internet de alta capacidade, o que permitiria, por si só, o melhoramento da infraestrutura de rede.

Não obstante, é também compartilhada, por estes, a premissa de que o estabelecimento de pedágio a ser pago pelas provedoras de aplicação levaria ao repasse de custos ao consumidor final, que se oneraria duplamente pelo mesmo serviço.

Sob a mesma opinião, a Associação Brasileira de Provedores de Internet e Telecomunicações (Abrint) defende que o debate estabelecido pela Anatel se sustentaria em falsas premissas relacionadas à existência de obstáculos à continuidade da prestação do serviço de telecomunicações no Brasil.

Desse modo, defende a ampla capacidade da rede e atribui qualquer defeito na prestação de serviço de conexão aos servidores de rede.

Com ainda maior ênfase na prejudicialidade da prática e compartilhando do mesmo raciocínio, a Coordenadora Geral de Saúde e Comunicações do Ministério da Fazenda, Marina Cavalcanti, em painel de debate do tema no 15º Encontro Nacional da Abrint, realizado no ano de 2024, discorreu sobre a dificuldade de estabelecimento de parâmetros para fixação de eventual tarifa sobre o consumo de rede, bem como sobre o impacto desta nos modelos de negócio a serem adotados pelos provedores de aplicação e nas barreiras existentes à entrada de novos *players* no mercado em questão.

Portanto, verifica-se, no cenário brasileiro, a existência de uma tendência à proibição da prática, por meio da iniciativa legislativa, e, ao mesmo tempo, o apontamento, por meio de representantes do setor privado, da necessidade de que a melhoria na infraestrutura do serviço de telecomunicações acompanhe o crescimento exponencial do tráfego na rede, sem, necessariamente, estabelecer, para isso, novas tarifas.

De toda forma, tem-se que nenhuma das iniciativas mencionadas encerra ou encerrará o debate, justamente em virtude de este não se restringir ao âmbito nacional, já que os principais provedores de aplicação mencionados como grandes consumidores de dados constituem empresas estrangeiras, cuja prestação de serviços se desenvolve a nível global.

Logo, é imprescindível que o Brasil, assim como toda a comunidade internacional, busque, para a resolução da discussão, um debate aberto, plural e extraterritorial, já que a rede mundial de computadores não tem fronteiras estabelecidas e as soluções a ela aplicadas não tem eficácia se adstritas a um país ou a um território.

6 PREVISÕES E CONCLUSÕES

Como visto ao longo do presente artigo, a temática do *fair share* é alvo dos mais diversos debates, seja por parte da comunidade internacional, dos órgãos governamentais brasileiros ou em eventos e discussões promovidas por membros e organizações representativas do setor privado.

Isso decorre do fato de que a legitimação da prática e do estabelecimento da tarifa de *fair share* têm reflexos nos mais diversos âmbitos: econômico, social e normativo.

No âmbito econômico, por sua vez, a imposição do pedágio pelo tráfego de dados na internet pode vir a influenciar o modelo de negócios a ser adotado pelos provedores de aplicação, o que acarretaria em entraves à oferta de seus produtos no território nacional.

Ora, se tiverem que redimensionar seus custos de infraestrutura para competição no mercado brasileiro, estas plataformas podem optar pelo encarecimento dos serviços ou até mesmo pela cessação do fornecimento destes no Brasil.

De maneira ainda mais importante, o estabelecimento de tarifa pela remessa de

grandes volumes de dados pode significar a imposição de importante barreira de entrada no mercado, o que pode obstar o surgimento de novos provedores de aplicação locais, bem como afastar a vinda de outros *players* para o país.

Logo, o *fair share* enquanto nova tarifa pode acarretar em um óbice à livre concorrência e à inovação na rede, o que traz importante preocupação quanto a repercussão deste na ordem econômica brasileira.

Em se tratando do impacto social da temática, tem-se que o custo extra imposto às plataformas pelo tráfego de dados na rede pode e muito provavelmente deverá ser repassado ao consumidor final do serviço, o que incorrerá em dupla cobrança – clara violação ao Código de Defesa do Consumidor – e, de maneira ainda mais grave, pode significar a redução do acesso à diversidade de conteúdos na internet, o encarecimento da contratação dos planos de banda e, por conseguinte, a exclusão digital.

Não suficiente, é importante destacar, ainda, os diversos gargalos existentes na instituição do *fair share*, que, por sua vez, impedem o seu estabelecimento de forma segura no contexto regulatório brasileiro.

São eles: a inexistência de definição precisa para o termo *heavy users*, o que impede a identificação clara dos sujeitos da regulação; a dificuldade de estabelecimento de parâmetros e critérios para tarifação do tráfego de dados; os limites da competência da Anatel para regulação e o enquadramento dos serviços de conexão como *essential facilities*.

Primeiramente, tem-se que a definição dos sujeitos da regulação, os chamados grandes usuários, é imprescindível para a restrição do alcance de eventual tarifa estabelecida para o uso das conexões de rede. Isso porque somente àqueles cujo volume de dados seja considerado exacerbado será imposta a obrigação pecuniária.

No entanto, verifica-se que a escassez de características comuns a serem atribuídas a estes *players* impede a sua qualificação sob um único conceito, uma vez que a única semelhança – o intenso tráfego de dados – constitui aspecto cuja vagueza impede o estabelecimento de definição justa e coerente.

Afinal, o mero enquadramento das empresas já conhecidas como *Big Techs* como *heavy users* acaba por impor a estas um tratamento discriminatório, inclusive perante novos *players* que adentrem o mercado com o mesmo modelo de negócios.

Além disso, a quantificação do volume de dados a ser considerado oneroso o

suficiente para justificar a imposição de tarifa é pouco tangível, já que vigente, inclusive, a proibição aos provedores de conexão de guardar os registros de acesso a aplicações de internet¹³.

Logo, mostra-se extremamente prejudicado o estabelecimento de definições concretas a embasar a determinação ou a especificação daqueles perante os quais poderia ser estabelecida a tarifa a título de *fair share*.

Quanto à competência da agência reguladora para a tratamento normativo do tema, mostra-se necessário ressaltar a distinção criada pela Lei Geral de Telecomunicações entre serviços de telecomunicações e serviços de valor adicionado, o que acaba por restringir a competência regulamentar da Anatel.

Dessa maneira, a atuação da Anatel deve se restringir ao setor das telecomunicações e aos agentes que nele se enquadram, o que exclui os SVAs e impede, portanto, que a mesma crie normas que se direcionem aos provedores de aplicação.

Para além dos limites de competência da Anatel, existem diferenças estruturais entre os serviços prestados por estes agentes, o que acaba por criar uma relação de dependência entre eles: os serviços de valor adicionado são realizados sobre a infraestrutura das redes de telecomunicações, de modo que dependem, para sua ocorrência, da capacidade dos usuários finais, que seriam os consumidores, de acessar os seus produtos por meio do acesso fornecido pelas operadoras de telecomunicações.

Logo, é possível, no mínimo, a cogitação do enquadramento dos serviços prestados pelos provedores de telecomunicação como essenciais às atividades realizadas pelos provedores de aplicação, o que resta, inclusive, assegurado no art. 61, p. 2^o¹⁴ da Lei Geral de Telecomunicações.

13. Art. 14. Na provisão de conexão, onerosa ou gratuita, é vedado guardar os registros de acesso a aplicações de internet. (BRASIL, 2014)

14. Art. 61. Serviço de valor adicionado é a atividade que acrescenta, a um serviço de telecomunicações que lhe dá suporte e com o qual não se confunde, novas utilidades relacionadas ao acesso, armazenamento, apresentação, movimentação ou recuperação de informações. (...) § 2º É assegurado aos interessados o uso das redes de serviços de telecomunicações para prestação de serviços de valor adicionado, cabendo à Agência, para assegurar esse direito, regular os condicionamentos, assim como o relacionamento entre aqueles e as prestadoras de serviço de telecomunicações. (BRASIL, 1997)

Sob esta lógica, portanto, a doutrina das *essential facilities*, que tem suas origens atreladas à jurisprudência norte americana, ensina que seria obrigatório o compartilhamento ou o franqueamento do acesso a estes bens essenciais para promoção da concorrência em um mercado.

Em outras palavras, não poderia ser vedado ou impedido, aos SVAs, o acesso aos serviços de telecomunicações, já que estes seriam essenciais à atividade praticada por aqueles.

Para correta compreensão do tema, no entanto, é imprescindível importar o precedente estudado por Maria Izabel Gomes Sant’Anna de Araújo¹⁵ (ARAUJO, 2020): *MCI Communications case*, que foi julgado no ano de 1983, pela Corte de Apelação do 7º Distrito dos Estados Unidos da América, e definiu quatro requisitos para o enquadramento do serviço no conceito de *essential facilities*. São os seguintes: o controle, por um *player* com poder de mercado, da estrutura essencial; a impossibilidade física ou econômica de duplicação da estrutura por parte dos concorrentes; a recusa por parte do detentor da estrutura do fornecimento de acesso a concorrentes e a possibilidade de liberação do acesso à estrutura sem a ocorrência de dano.

Pois bem.

Em analogia para a conversão e adaptação destes requisitos à realidade dos serviços de telecomunicações no Brasil, pode-se dizer que os SVAs, como já dito, certamente têm a oferta de seus produtos no mercado condicionada ao uso da estrutura de conexão fornecida pelas operadoras de rede.

De maneira ainda mais certa, é possível admitir que estes atuam em um âmbito onde o mercado de oferta de conexão de rede é dominado por poucos *players*, que a duplicação da infraestrutura de conexão por estes para fornecimento direto de seus serviços é essencialmente onerosa e desarrazoada, vez que foge ao seu escopo de negócios, e que, no mínimo, se admite que o uso da estrutura fornecida pelas operadoras de rede ocorre sem a geração de dano não indenizado, vez que se baseia em relação onerosa custeada pelos consumidores finais dos serviços.

15. Breve análise sobre a essential facilities doctrine. In: PINHEIRO, Armando Castelar; PORTO, Antônio José Maristrello; ABRAHAM, Marcus; SAMPAIO, Patrícia Regina Pinheiro. FGV Direito Rio. Rio de Janeiro. 2020

Como consequência disso, a imposição de tarifa extra aos SVAs para uso do serviço fornecido pelas operadoras de rede constitui, em suma, a imposição de óbice e eventualmente a negação de acesso a bens essenciais, o que configura, conforme definido na Seção 2 do *Sherman Act*¹⁶, monopólio ilegal ou abuso de domínio.

Nesse exato sentido, o artigo 146, inciso III¹⁷ da Lei de Telecomunicações estabelece que o direito de propriedade sobre as redes deve estar condicionado ao cumprimento de sua função social.

Portanto, como mostrado ao longo dos tópicos e como exposto nesta abordagem final, o estabelecimento do *fair share* no contexto brasileiro normativo e econômico em que é cogitado se mostra extremamente prejudicial e desarrazoado e contraria o princípio da neutralidade de rede, que resta preconizado no Marco Civil da Internet.

É legítima, no entanto, a preocupação com o incremento da infraestrutura das conexões de rede, mas entende-se que o eventual crescimento no tráfego de dados na rede também está amparado pelo investimento realizado, inclusive, pelos próprios provedores de aplicação, em *data centers*, cabos submarinos e terrestres de conexão e redes de entrega¹⁸, além de não justificar, por si só, o estabelecimento de onerosa tarifa com base em vagas premissas.

Finalmente, mostra-se relevante a pluralidade do debate, já que, como dito, o *fair share* tem repercussões econômicas, jurídicas e sociais, o que torna imprescindível o envolvimento dos diversos setores nas tratativas da temática.

16. (EUA, DEPARTMENT OF JUSTICE, 2022). *Sherman Act* é a Lei Antitruste norte americana que, como importante referência internacional, traz princípios acerca da livre concorrência. Disponível em: <https://www.justice.gov/archives/atr/competition-and-monopoly-single-firm-conduct-under-section-2-sherman-act-chapter-1> Acesso em: 26/06/2024

17. Art. 146. As redes serão organizadas como vias integradas de livre circulação, nos termos seguintes: (...) III - o direito de propriedade sobre as redes é condicionado pelo dever de cumprimento de sua função social. (BRASIL, 1997)

18. Entre 2018 e 2021, esses investimentos anuais aumentaram em 50% em comparação ao período de 2014 a 2017, alcançando uma média de 120 bilhões de dólares por ano em infraestrutura (ANALYSYS MASON, 2022)

REFERÊNCIAS

- ANATEL. *Tomada de Subsídio n. 13. Item 6 da Agenda Regulatória da Anatel para o Biênio 2023-2024 – Regulamento De Deveres Dos Usuários. Realizada em março de 2023*. Disponível em: <https://apps.anatel.gov.br/ParticipaAnatel/VisualizarTextoConsulta.aspx?TelaDeOrigem=3&ConsultaId=10120> Acesso em: 16/05/2024
- ANATEL. *Tomada de Subsídio n. 26. Item 6 da Agenda Regulatória da Anatel para o Biênio 2023-2024 – Regulamento De Deveres Dos Usuários. Realizada em janeiro de 2024*. Disponível em: <https://apps.anatel.gov.br/ParticipaAnatel/VisualizarTextoConsulta.aspx?TelaDeOrigem=2&ConsultaId=20202> Acesso em: 19/06/2024
- ARAÚJO, Maria Izabel Gomes Sant’anna de. *Breve análise sobre a essential facilities doctrine*. In: PINHEIRO, Armando Castelar; PORTO, Antônio José Maristrello; ABRAHAM, Marcus; SAMPAIO, Patrícia Regina Pinheiro. FGV Direito Rio. Rio de Janeiro. 2020
- BELLI, Luca; DE FILIPPI, Primavera. *Net Neutrality Compendium: Human Rights, Free Competition and the Future of the Internet*. New York: Springer, 2016.
- BRASIL. *Lei 9.472, de 16 de julho de 1997. Dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador e outros aspectos institucionais, nos termos da Emenda Constitucional nº 8, de 1995*. Diário Oficial da União, Brasília, DF, 16 de julho de 1997. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9472.htm. Acesso em: 30/05/2024.
- BRASIL. *Lei nº 12.965, de 23 de abril de 2014. Diário Oficial da União, Brasília, DF, 24 abr. 2014*. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 01/06/2024.
- CADE. *NOTA TÉCNICA Nº 34/2017/CGAA4/SGA1/SG/CADE*. Disponível em: https://sei.cade.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?DZ2uWeaYicbuRZEF.... Acesso em: 06/06/2024
- COLANGELO, Giuseppe, *Fair Share of Network Costs and Regulatory Myopia: Learning from Net Neutrality Mistakes* (July 18, 2023). Forthcoming in Law, Innovation and Technology, ICLE Research Paper, Available at SSRN: <https://ssrn.com/abstract=4452280> or <http://dx.doi.org/10.2139/ssrn.4452280>
- CONGRESSO NORTE-AMERICANO. *Fair Contributions Act. 2023-2024*. Disponível em: <https://www.congress.gov/bill/118th-congress/senate-bill/856> Acesso em: 02/06/2024
- CONGRESSO NORTE-AMERICANO. *26 Stat. 209, 15 U.S.C. §§ 1–7. Competition And Monopoly: Single-Firm Conduct Under Section 2 Of The Sherman Act: Chapter 1*. 1980. Disponível em: <https://www.justice.gov/archives/atr/competition-and-monopoly-single-firm-conduct-under-section-2-sherman-act-chapter-1>. Acesso em: 22/06/2024
- CONSELHO DIGITAL. *Resposta a tomada de subsídios 26: Regulamento de deveres dos usuários*. p. 131, maio 2024. Disponível em: <https://conselhodigital.org.br/wp->

- content/uploads/2024/05/CONSELHO-DIGITAL-Tomada-de-Subsi%CC%81dios-26-Anatel-Deveres-de-usua%CC%81rios.pdf. Acesso em: 27/06/2024
- GRAEF, Inge. *Essential facility*, Global Dictionary of Competition Law, Concurrences, Art. N° 12256. Disponível em: <https://www.concurrences.com/en/dictionary/essential-facility>. Acesso em: 29/06/2024
- JITSUZUMI, Toshiya, *Economic Impact of Asymmetric Paid Peering: Implications of the Netflix vs. SK Broadband Dispute* (August 1, 2022). Available at SSRN: <https://ssrn.com/abstract=4178217> or <http://dx.doi.org/10.2139/ssrn.4178217>
- KOPF, Wolfgang. *Cologne Regional Court Rules: Meta Must Pay for Network Usage – An Important Step for “Fair Share”*. Disponível em: <https://www.telekom.com/en/company/management-unplugged/details/meta-must-pay-for-the-use-of-the-networks-1066682>. Acesso em: 21 jun.
- LEITE, George Salomão; LEMOS, Ronaldo. *Marco Civil da Internet*. São Paulo: Atlas, 2014.
- MARSDEN, Christopher. *Net Neutrality: Towards a Co-Regulatory Solution*. Bloomsbury Publishing, 2010.
- NERY, Carmen. *Em 2022, streaming estava presente em 43,4% dos domicílios com TV | Agência de Notícias*. Disponível em: <https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/38306-em-2022-streaming-estava-presente-em-43-4-dos-domicilios-com-tv>. Acesso em: 09/06/2024.
- OECD Competition Committee, *Refusals to Deal* (DAF/COMP(2007)46, September 2009).
- PARENTONI, Leonardo. *Neutralidade de rede: mudanças na infraestrutura da internet e como isso influencia na sua vida*. Revista Jurídica da Presidência. 19. 560. 10.20499/2236-3645.RJP2018v19e119-1365, 2018.
- PEREIRA NETO, Caio Mario da Silva; et al. *A compatibilidade da prática de zero-rating com a previsão de neutralidade de rede*. Revista Direito GV. São Paulo: Direito GV, v. 15, n. 33, p. 01-32, mai./ago. 2019.
- PRESCOTT, Roberta. *Debate sobre fair share avança e entidades da sociedade civil se posicionam contra*. Disponível em: <https://www.abranet.org.br/Noticias/Debate-sobre-fair-share-avanca-e-entidades-da-sociedade-civil-se-posicionam--contra-4528.html?UserActiveTemplate=mobile%252Csite%25252Csite&from%255Finfo%255Findex=881>. Acesso em: 16 jun. 2024.
- PROJETO DE LEI 469/24. *Acrescenta o art. 90-A à Lei no 12.965, de 23 de abril de 2014 (Marco Civil da Internet), para proibir que provedores de conexão de internet instituem cobrança direcionada aos provedores de aplicações de internet por geração de tráfego de dados*. Ano de 2024. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2390084&filename=Tramitacao-PL%20469/2024. Acesso em: 15/06/2024
- RAMOS, Pedro Henrique Soares. *Arquitetura da rede e regulação: a neutralidade da rede no Brasil*. 2015. 218 f. *Dissertação* (Mestrado em Direito da Escola de Direito da Fundação Getúlio Vargas)

– FGV, São Paulo, 2015.

UNIÃO EUROPEIA. *O futuro do setor das comunicações eletrônicas e das suas infraestruturas - Shaping Europe's digital future*. Disponível em: <<https://digital-strategy.ec.europa.eu/pt/consultations/future-electronic-communications-sector-and-its-infrastructure>>. Acesso em: 16 jun. 2024.

URUPÁ, M. *Debate sobre fair share se fundamenta em falsas premissas, afirma Abrint*. Disponível em: <<https://teletime.com.br/12/06/2024/debate-sobre-fair-share-se-fundamenta-em-falsas-premissas-afirma-abrint/>>. Acesso em: 2 jul. 2024.

WU, Tim. *Network Neutrality, Broadband Discrimination*, 2 J. on Telecomm. & High Tech. L. 141, 2003.

IV

PROVEDORES DE SERVIÇO (ISP'S): ESPÉCIES,
GUARDA DE REGISTROS E RESPONSABILIDADE CIVIL

DEVERES JURÍDICOS DOS PROVEDORES DE INTERNET E GUARDA DE REGISTROS

Lorenzo Antonini Itabaiana

Mestrando em Direito e Tecnologia pela UFMG. Bacharel em Direito pela UFMG.
Advogado. E-mail: lorenzzoantonini@gmail.com

José Luiz de Moura Faleiros Júnior

Doutor em Direito pela USP e pela UFMG. Mestre e Bacharel em Direito pela UFU.
Advogado. E-mail: josefaleirosjr@outlook.com

DOI: <https://doi.org/10.59224/dti7.ch6>

Resumo: Os provedores de internet têm deveres jurídicos fundamentais na guarda de registros e na facilitação de negócios inovadores. Esses deveres incluem a proteção de dados pessoais, a manutenção de registros de atividades de usuários para investigações legais e o cumprimento de regulamentações de privacidade. A responsabilidade que exsurge desses deveres se estende à garantia de segurança e confidencialidade das informações armazenadas. Neste trabalho, analisar-se-á quem são os provedores de internet, e as principais obrigações relativas à guarda dos registros de conexão e aplicação, assegurando um ambiente digital seguro e propício ao desenvolvimento de novos negócios e serviços on-line.

Palavras-chave: deveres jurídicos; provedores de internet; proteção de dados; inovação tecnológica.

Abstract: Internet providers have fundamental legal duties in record keeping and facilitating innovative businesses. These duties include protecting personal data, maintaining user activity logs for legal investigations, and complying with privacy regulations. The responsibilities arising from these duties extend to ensuring the security and confidentiality of stored information. This paper will analyze who internet providers are, and the main obligations regarding the safe-keeping of connection and application logs, ensuring a safe digital environment conducive to the development of new online businesses and services.

Keywords: legal duties; internet providers; data protection; technological innovation.

SUMÁRIO: Introdução. 1. Os provedores de internet e suas classificações; 1.1. Definição de Serviços de Telecomunicações e Valor Adicionado; 1.2. *Digital Millennium Copyright Act* (DMCA); 1.3. Categorização Infraestrutural (1999); 1.4. Categorização Finalística (2001); 1.5. Categorização Contextual (2010); 1.6. Tipologia de Provedores de Serviços; 2. Deveres de guarda de registros e contextos específicos; 3. Endereço IP e portas lógicas; 3.1. Internet Protocol (IP); 3.2. Portas lógicas; Conclusão; Referências.

INTRODUÇÃO

Antes da promulgação do Marco Civil da Internet (Lei nº 12.965/2014), os provedores de internet no Brasil eram classificados, conforme a legislação vigente, em duas categorias principais: prestadores de serviços de telecomunicações e provedores de aplicação de internet. Essa categorização estava baseada na Lei Geral de Telecomunicações (Lei nº 9.472/1997), que impunha uma série de obrigações aos prestadores de serviços, incluindo a obtenção de concessões e a prestação de contas ao órgão regulador. A ausência de uma regulamentação específica para a internet gerava insegurança jurídica, refletida em decisões judiciais variadas e muitas vezes contraditórias. Diante do surgimento de novos negócios inovadores e novas tecnologias de telecomunicações, passou a ser urgente responder à pergunta: quem são os intermediários da internet?¹

Com a promulgação do Marco Civil da Internet, foram estabelecidos princípios fundamentais como a neutralidade da rede, a proteção de dados e a privacidade, além de definir claramente as responsabilidades dos provedores de internet pelo conteúdo gerado por terceiros. A lei trouxe uma nova estrutura regulatória que buscava equilibrar a liberdade de expressão com a proteção dos direitos dos usuários. Por fim, delimitou os provedores em apenas duas categorias.

Além das legislações específicas, este estudo também examina diferentes propostas teóricas de categorização dos provedores de internet, como as de Pedro Alberto

1. Parafraseando Giancarlo Frosio: FROSIO, Giancarlo. Mapping Online Intermediary Liability. In: FROSIO, Giancarlo (ed.). *The Oxford Handbook of Online Intermediary Liability*. Oxford: Oxford University Press, 2020, p. 6.

de Miguel Asensio², Marcel Leonardi³, Lawrence Lessig⁴, e Tim Wu⁵. Essas categorizações ajudam a contextualizar as funções e responsabilidades dos provedores dentro do ecossistema digital mais amplo. A metodologia qualitativa permite uma análise aprofundada dessas propostas, comparando-as com a realidade jurídica brasileira e destacando as particularidades e desafios enfrentados pelos provedores de internet

2. Em 2000, o professor de Miguel Asensio escreveu uma importante monografia sobre o Direito Privado e suas correlações com os avanços da Internet (a primeira edição foi publicada em Madrid pela editora Civitas). A obra, que se tornou um clássico na literatura jurídica, passou por várias edições. A recente sexta edição, publicada em 2022, oferece uma atualização completa e inclui novos tópicos e problemas. A obra cresceu de 1150 para 1612 páginas desde a edição de 2015, refletindo a rápida evolução do setor. Este livro é uma referência essencial para juristas que lidam com questões jurídicas privadas na internet, abordando problemas atuais, tendências e jurisprudência com análise rigorosa e crítica. Não obstante, já na edição inaugural, Pedro de Miguel Asensio tratou de propor uma classificação dos provedores (*"Régimen jurídico de los prestadores de servicios de lasociedad de lainformación"*), que é de crucial estudo até os dias atuais. Cf. DE MIGUEL ASENSIO, Pedro A. *Derecho Privado de Internet*. 6. ed. Cizur Menor (Navarra): Civitas, 2022.
3. A obra do professor Marcel Leonardi deve ser sempre referenciada, pois foi ele o primeiro a analisar a responsabilidade dos provedores sob a perspectiva do direito brasileiro, diferenciando claramente entre os diversos tipos de provedores (de acesso, de conteúdo, de *backbone*) e suas respectivas responsabilidades. Sua obra foi pioneira ao abordar a necessidade de regulamentação específica para provedores de serviços de internet, destacando os desafios jurídicos e a importância da segurança jurídica no ambiente digital. Cf. LEONARDI, Marcel. *Responsabilidade civil dos provedores de serviços de Internet*. São Paulo: Juarez de Oliveira, 2005.
4. O professor Lawrence Lessig foi o primeiro a argumentar que o código de *software* é uma estrutura de poder, influenciando como as interações ocorrem na internet. Ele discutiu como a arquitetura da internet pode ser regulada para proteger direitos fundamentais e promover uma internet aberta e justa. Seu trabalho enfatizou a importância de políticas que considerem as influências técnicas no comportamento dos provedores e usuários, contribuindo para a discussão sobre a necessidade de regulação e classificação dos provedores de internet. Cf. LESSIG, Lawrence. *Code and Other Laws of Cyberspace*. 2. ed. Nova York: Basic Books, 2006.
5. Wu explorou a história dos monopólios de comunicação e como eles influenciam o controle e a inovação na internet. Ele introduziu o conceito de "ciclo de Wu", pelo qual indústrias de comunicação alternam entre períodos de abertura e fechamento. Sua análise destacou a importância de manter a neutralidade da rede e a diversidade de provedores, alertando contra a concentração de poder e a necessidade de políticas que incentivem a competição e protejam os consumidores. Cf. WU, Tim. *The Master Switch: The Rise and Fall of Information Empires*. Nova York: Vintage, 2010.

na atualidade.

Este artigo busca oferecer uma compreensão das responsabilidades jurídicas específicas dos provedores de internet, considerando o contexto histórico, mudanças legislativas e teóricas. Utilizando o método dedutivo, esta pesquisa será desenvolvida com foco em estabelecer como essas normas foram implementadas e as implicações jurídicas decorrentes para os provedores de internet no Brasil. A abordagem qualitativa permitirá uma análise detalhada das implicações dessas responsabilidades, contribuindo para um entendimento mais claro e sistemático das obrigações dos provedores de internet no Brasil. Serão examinadas as principais leis, decisões judiciais e classificações teóricas, com foco nas obrigações de guarda de registros.

Para compreender quem são os provedores de internet e suas principais obrigações, vamos, na primeira parte, detalhar as correntes sobre as classificações dos provedores de internet. Em um segundo momento, abordaremos o registro de logs de acesso por esses provedores, tendo o Marco Civil da Internet como principal referência⁶. Apresentaremos diversos pontos de reflexão sobre esses temas, buscando respondê-los de forma sucinta, sem pretensão de esgotar todas as questões levantadas. Para aprofundar, trataremos sobre a porta lógica e os principais debates relacionados ao armazenamento de logs por provedores de internet. Por fim, destacamos que não pretendemos discutir a responsabilidade dos provedores por danos a terceiros nem a mediação de conteúdo.

1. OS PROVEDORES DE INTERNET E SUAS CLASSIFICAÇÕES

Antes da promulgação do Marco Civil da Internet (Lei nº 12.965/2014)⁷, os

-
6. É sempre conveniente lembrar o contexto histórico para a análise em questão, pois, tal como diz o professor Newton De Lucca, “o Marco Civil da Internet foi, efetivamente, fruto de um longo debate nacional, tanto na Câmara dos Deputados, na qual tramitou por cerca de três anos, como na sociedade em geral, tendo havido, inegavelmente, ampla participação da sociedade civil, como se pôde verificar pelas várias consultas públicas realizadas nas diversas localidades do Brasil”. DE LUCCA, Newton. Marco Civil da Internet - uma visão panorâmica dos principais aspectos relativos às suas disposições preliminares. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coord.). *Direito & Internet III: Marco Civil da Internet (Lei nº 12.965/2014)*. São Paulo: Quartier Latin, 2015, t. I, p. 27.

7. Permanece atual a reflexão de Demi Getschko: “Há diversas formas de se analisar o significado do

provedores de internet no Brasil eram categorizados como prestadores de serviços de telecomunicações ou provedores de aplicação de internet, conforme a legislação vigente. Os prestadores de serviços de telecomunicações eram regulamentados pela Lei Geral de Telecomunicações (Lei nº 9.472/1997), que impunha obrigações rigorosas, incluindo a obtenção de concessões, permissões ou autorizações para operar, a realização de investimentos em infraestrutura e a prestação de contas ao órgão regulador. Além disso, o Código de Defesa do Consumidor (Lei nº 8.078/1990) já desempenhava um papel importante na proteção dos usuários da rede, usualmente em discussões relacionadas a defeitos na prestação de serviços no comércio eletrônico⁸.

1.1. Definição de Serviços de Telecomunicações e Valor Adicionado

Neste subtópico, abordar-se-á a definição dos serviços de telecomunicações e de valor adicionado conforme previstos na Lei Geral de Telecomunicações (Lei nº 9.472/1997). Em linhas gerais, os serviços de telecomunicações envolvem a transmissão e recepção de informações por diversos meios, enquanto os serviços de valor adicionado introduzem novas utilidades sem se confundir com os serviços de telecomunicações, classificando seus provedores como usuários desses serviços, com direitos e deveres inerentes.

Sobre o tema, comenta Adalberto Simão Filho:

“Após a adoção das medidas necessárias para o atendimento do interesse público e desenvolvimento das telecomunicações brasileiras, por parte da

Marco Civil da Internet no Brasil. Pode-se, por exemplo, tratá-lo por seu caráter legal, como um componente jurídico novo que é, e que interage com todo o estamento existente. Certamente haveria muito interesse em examinar essa interação em detalhe. O Marco também pode ser objeto de análise pela ótica do humanismo, das consequências de sua aplicação na sociedade, dos efeitos de sua evolução e de seus impactos sobre os diferentes segmentos da atividade, sobre a economia, sobre as transações diárias e sobre seu papel na proteção dos direitos individuais”. GETSCHKO, Demi. As origens do Marco Civil da Internet. In: LEITE, George Salomão; LEMOS, Ronaldo (coord.). *Marco Civil da Internet*. São Paulo: Atlas, 2014. p. 12.

8. TOMASEVICIUS FILHO, Eduardo. O Marco Civil da Internet e as liberdades de mercado. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coord.). *Direito & Internet III: Marco Civil da Internet (Lei nº 12.965/2014)*. São Paulo: Quartier Latin, 2015, t. II. p. 50-51.

ANATEL, com a consequente criação da rede de infra-estrutura que possibilitou o cumprimento do princípio da universalização, passam os competidores a operar maciçamente junto ao mercado com vistas a prestar os serviços objeto do contrato de concessão firmado, atendendo aos condicionantes e limitadores geradores de ampla e justa competição, bem como buscando a justa equivalência entre esta prestação de serviços e a remuneração ideal. Neste cenário compete ao Poder Público atuar não só para propiciar a livre competição, como também para corrigir os efeitos de uma competição imperfeita, reprimindo as infrações da ordem econômica, à luz do art. 170 da Constituição Federal e do art. 6º da Lei Geral de Telecomunicações”⁹.

A Lei Geral de Telecomunicações (Lei nº 9.472/1997) desempenhou um papel crucial no pioneirismo regulatório brasileiro ao definir categorias de serviços e provedores, facilitando o avanço das telecomunicações e pavimentando o caminho para a definição de provedores de internet e seus deveres.

O artigo 60 estabelece que o serviço de telecomunicações é um conjunto de atividades que permite a oferta de telecomunicações, abrangendo a transmissão, emissão ou recepção de símbolos, caracteres, sinais, escritos, imagens, sons ou informações por qualquer meio eletromagnético¹⁰. Além disso, define a estação de telecomunicações como o conjunto de equipamentos necessários para a realização dessas atividades.

O artigo 61, por sua vez, distingue os serviços de valor adicionado, que são atividades que acrescentam novas utilidades a um serviço de telecomunicações, mas não

9. SIMÃO FILHO, Adalberto. Do contrato de concessão para serviços de telecomunicações à telefonia IP-VoIP: reflexos nos direitos transindividuais. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto (coord.). *Direito & Internet II: aspectos jurídicos relevantes*. São Paulo, 2008. p. 113.

10. “Art. 60. Serviço de telecomunicações é o conjunto de atividades que possibilita a oferta de telecomunicação. § 1º Telecomunicação é a transmissão, emissão ou recepção, por fio, radioeletridade, meios ópticos ou qualquer outro processo eletromagnético, de símbolos, caracteres, sinais, escritos, imagens, sons ou informações de qualquer natureza. § 2º Estação de telecomunicações é o conjunto de equipamentos ou aparelhos, dispositivos e demais meios necessários à realização de telecomunicação, seus acessórios e periféricos, e, quando for o caso, as instalações que os abrigam e complementam, inclusive terminais portáteis”.

se confundem com este, classificando seu provedor como usuário do serviço de telecomunicações¹¹. Esse dispositivo assegura o uso das redes de telecomunicações para a prestação de serviços de valor adicionado, permitindo a regulação pela Agência para garantir direitos e deveres entre provedores e prestadoras de serviço¹².

Essas definições foram pioneiras ao fornecer uma base regulatória clara, permitindo a distinção entre diferentes tipos de serviços e criando um ambiente regulatório que favoreceu a inovação e o desenvolvimento das telecomunicações no Brasil. Essa clareza regulatória foi fundamental para o crescimento do setor e para a futura categorização dos provedores de internet, ajudando a definir suas responsabilidades e obrigações de maneira mais precisa.

1.2. *Digital Millennium Copyright Act (DMCA)*

O *Digital Millennium Copyright Act (DMCA)*, promulgado em 1998 nos Estados

11. “Art. 61. Serviço de valor adicionado é a atividade que acrescenta, a um serviço de telecomunicações que lhe dá suporte e com o qual não se confunde, novas utilidades relacionadas ao acesso, armazenamento, apresentação, movimentação ou recuperação de informações. § 1º Serviço de valor adicionado não constitui serviço de telecomunicações, classificando-se seu provedor como usuário do serviço de telecomunicações que lhe dá suporte, com os direitos e deveres inerentes a essa condição. § 2º É assegurado aos interessados o uso das redes de serviços de telecomunicações para prestação de serviços de valor adicionado, cabendo à Agência, para assegurar esse direito, regular os condicionamentos, assim como o relacionamento entre aqueles e as prestadoras de serviço de telecomunicações”.
12. O fomento à atividade econômica dos provedores de internet não deixou de ser observado em relação aos serviços de valor adicionado. Após sucessivos questionamentos, consolidou-se na Súmula 334 do Superior Tribunal de Justiça o entendimento de que o Imposto sobre Circulação de Mercadorias e Serviços - ICMS não incide sobre os serviços dos provedores de acesso à internet. Esse entendimento é significativo pois diferencia os serviços de acesso à internet dos serviços de comunicação, que são tributáveis pelo ICMS. A súmula reflete o reconhecimento de que o fornecimento de acesso à internet é uma atividade distinta, essencial para a democratização do uso da rede e para o desenvolvimento do setor de tecnologia da informação no Brasil, aliviando a carga tributária sobre os provedores e incentivando a expansão do acesso à internet, não atrelando o disposto no artigo 2º da Lei Complementar 87/1996. Sobre o tema, conferir QUEIROZ, Renata CapriolliZocatelli; BENICIO, Mariane Menezes; LATTANZIO, Daniel Zonzini. A não incidência do ISS e do ICMS sobre o serviço de valor adicionado. *Revista Foco*, Curitiba, v. 16, n. 2, p. 1-13, 2023.

Unidos, foi uma resposta ao aumento da pirataria na internet¹³. Esta legislação criou um "porto seguro" para provedores de serviços de internet (ISPs), isentando-os de responsabilidade pelo conteúdo gerado por terceiros, desde que removam o conteúdo infrator quando notificados pelos detentores dos direitos autorais. Embora facilite a operação dos ISPs, essa classificação é criticada por alguns detentores de direitos autorais, que argumentam que ela não oferece proteção suficiente para os criadores de conteúdo.

1.3. Categorização Infraestrutural (1999)

Lawrence Lessig, em seu livro "*Code and Other Laws of Cyberspace*" (2006), propôs uma classificação dos provedores de internet em quatro categorias: arquiteturais, reguladores, *marketmakers* e conjuradores. Esta categorização enfatiza as diversas funções e responsabilidades dos provedores dentro da infraestrutura da internet, bem como suas interações com regulamentações e transações comerciais. Lessig argumenta que os provedores arquiteturais são responsáveis pelo desenvolvimento e manutenção das infraestruturas tecnológicas que possibilitam a comunicação e o tráfego de dados na internet¹⁴. Eles criam a espinha dorsal que sustenta toda a rede, incluindo hardware, protocolos e software que definem como as informações são transmitidas e recebidas.

Os provedores reguladores, por sua vez, desempenham um papel crucial na definição das normas e políticas que governam o uso da internet. Eles trabalham em estreita colaboração com governos e organizações internacionais para estabelecer regulamentações que assegurem a segurança, privacidade e acessibilidade na rede. Essas regulamentações podem incluir leis de proteção de dados, diretrizes de neutralidade da rede e normas de segurança cibernética, que são essenciais para o funcionamento harmonioso e seguro do ambiente digital. Os reguladores, portanto, são fundamentais para garantir que a internet continue a ser um espaço livre e seguro para

13. ESTADOS UNIDOS DA AMÉRICA. *Digital Millennium Copyright Act (DMCA)*. Public Law 105-304, 1998. Disponível em: <https://www.copyright.gov/legislation/dmca.pdf> Acesso em: 14 maio 2024.

14. LESSIG, Lawrence. *Code and Other Laws of Cyberspace*. 2. ed. Nova York: Basic Books, 2006, p. 88.

todos os usuários.

Finalmente, Lessig descreve os provedores como categorias que lidam diretamente com os aspectos econômicos e inovadores da internet. Os *marketmakers* facilitam as transações comerciais on-line, criando plataformas que conectam compradores e vendedores, e estabelecem os padrões para a troca de bens e serviços digitais. Eles desempenham um papel central na economia digital, promovendo o comércio eletrônico e a inovação empresarial¹⁵. Os conjuradores, por outro lado, são os inovadores que introduzem novas tecnologias e serviços que transformam a maneira como usamos a internet. Eles são responsáveis por avanços que podem mudar radicalmente o cenário digital, introduzindo novas funcionalidades e oportunidades para os usuários. Assim, Lessig destaca a complexidade e a interdependência das várias funções desempenhadas pelos provedores de internet, sublinhando a importância de cada categoria na construção e manutenção do ciberespaço.

1.4. Categorização finalística (2001)

Em 2000, Pedro Alberto de Miguel Asensio publicou a primeira edição de sua obra "*Derecho Privado de Internet*", que se tornou um clássico na literatura jurídica e passou por várias edições. A sexta edição, lançada em 2022, oferece uma atualização abrangente, incluindo novos tópicos e questões, expandindo seu conteúdo de 1150 para 1612 páginas desde a edição de 2015, refletindo a rápida evolução do setor. O autor divide os provedores de internet em quatro categorias principais: (i) provedores de rede; (ii) provedores de serviços de acesso; (iii) provedores de serviços de conteúdo; e (iv) provedores de serviços de aplicação¹⁶.

Desde a primeira edição, Pedro de Miguel Asensio propôs uma classificação dos provedores de serviços de informação, que continua a ser um estudo crucial até os dias atuais. Além das fontes já mencionadas, o autor analisa o *Digital Services Act*¹⁷ e

15. LESSIG, Lawrence. *Code and Other Laws of Cyberspace*. 2. ed. Nova York: Basic Books, 2006, p. 115.

16. DE MIGUEL ASENSIO, Pedro A. *Derecho Privado de Internet*. 6. ed. Cizur Menor (Navarra): Civitas, 2022. p. 315 *et seq.*

17. DE MIGUEL ASENSIO, Pedro A. *Derecho Privado de Internet*. 6. ed. Cizur Menor (Navarra): Civitas, 2022. p. 369 *et seq.*

a proposta de Lei de Mercados Digitais¹⁸. Destaca, ainda, o Regulamento (UE) 2019/1150, que estabelece regras para garantir a transparência e a equidade nos serviços de intermediação on-line, protegendo usuários e comerciantes contra práticas desleais, a Diretiva (UE) 2019/770, que regula contratos de fornecimento de conteúdos e serviços digitais, definindo direitos e obrigações para consumidores e fornecedores, enquanto a Diretiva (UE) 2019/790 harmoniza os direitos de autor no mercado único digital, abordando desafios do ambiente on-line para proteger criadores e distribuidores de conteúdo. Cita, ainda, a Lei 6/2020 da Espanha, que regula serviços eletrônicos de confiança, como assinaturas digitais, promovendo segurança e confiança nas transações eletrônicas. Além disso, as atualizações recentes da jurisprudência do TJUE e dos tribunais espanhóis fornecem interpretações e aplicações práticas das normas, influenciando a conformidade e a regulamentação dos provedores de serviços¹⁹.

Desde a primeira edição da obra, a categorização proposta por Asensio esclarece as diferentes responsabilidades e serviços oferecidos por cada tipo de provedor, permitindo uma compreensão mais profunda das suas funções dentro do ecossistema digital. Este livro é uma referência indispensável para juristas que lidam com questões jurídicas privadas na internet, abordando problemas atuais, tendências e jurisprudência com análise crítica e rigorosa. Desde a edição inaugural, Asensio propôs uma classificação dos provedores de serviços de informação, que continua sendo um estudo crucial até hoje. A análise do autor é dita “finalística”, porquanto baseada na inspiração que lhe proporcionou o regime de exoneração condicionada de responsabilidade para os intermediários on-line introduzido pela Diretiva 2000/31/CE. Nela, os artigos 12-14 foram inspirados na seção 5 da Lei Federal Alemã de Teleserviços (*Teledienstegesetz* ou TDG) e na seção 512 do *Digital Millennium Copyright Act* dos Estados Unidos da América (DMCA).

As regras de exoneração de responsabilidade, conhecidas como “*safe harbors*” (portos seguros), não visam determinar a responsabilidade dos intermediários on-

18. DE MIGUEL ASENSIO, Pedro A. *Derecho Privado de Internet*. 6. ed. Cizur Menor (Navarra): Civitas, 2022. p. 670 *et seq.*

19. DE MIGUEL ASENSIO, Pedro A. *Derecho Privado de Internet*. 6. ed. Cizur Menor (Navarra): Civitas, 2022. p. 815 *et seq.*

line, mas limitar as situações em que podem ser considerados responsáveis²⁰. No entanto, as condições para a exoneração de responsabilidade, como o requisito de atuação diligente previsto no artigo 6.1 do recente *Digital Services Act*²¹, especificam a diligência mínima esperada desses intermediários na prestação de seus serviços.

1.5. Categorização Contextual (2010)

Tim Wu, em "*The Master Switch: The Rise and Fall of Information Empires*", classifica os provedores de internet em cinco categorias: infraestrutura, hardware, software, conteúdo e aplicativos. Esta categorização posiciona os provedores dentro do ecossistema tecnológico mais amplo, destacando as interdependências entre os diversos componentes tecnológicos e suas implicações para a operação da internet²². Ao fazer isso, Wu oferece uma visão abrangente sobre como cada categoria contribui para o funcionamento geral da rede e como elas se interrelacionam para proporcionar uma experiência de usuário coesa e eficiente.

Os provedores de infraestrutura são responsáveis por fornecer a base física e tecnológica sobre a qual a internet é construída. Isso inclui cabos submarinos, data centers, torres de telecomunicações e outras instalações essenciais que garantem a conectividade global. Sem esta base sólida, o restante do ecossistema não poderia funcionar adequadamente. Os provedores de hardware, por sua vez, desenvolvem e fornecem os dispositivos e equipamentos necessários para acessar e utilizar a internet, como roteadores, modems, servidores e computadores. Esses componentes de hardware são vitais para traduzir os sinais transmitidos pela infraestrutura em dados utilizáveis para os usuários finais.

20. HERRERÍAS CASTRO, Laura. ¿Matar al mensajero? La responsabilidad de las redes sociales y los usuarios por difamación. *Revista d'Internet, Dret i Política*, Barcelona: Universitat Oberta de Catalunya, n. 40, p. 1-12, mar. 2024. p. 4.

21. UNIÃO EUROPEIA. *Regulamento (UE) 2022/2065 do Parlamento Europeu e do Conselho de 19 de outubro de 2022 relativo a um Mercado Único de Serviços Digitais e que altera a Diretiva 2000/31/CE (Digital Services Act)*. 2022. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32022R2065> Acesso em: 30 maio. 2024.

22. Cf. WU, Tim. *The Master Switch: The Rise and Fall of Information Empires*. Nova York: Vintage, 2010.

1.6. Tipologia de Provedores de Serviços

Marcel Leonardi, em "Responsabilidade Civil dos Provedores de Serviços de Internet" (2005), propôs uma tipologia para os provedores de serviços de internet no Brasil, anterior ao Marco Civil da Internet. Leonardi sugere classificações como provedores de *backbone*²³, de acesso, de correio eletrônico, de hospedagem e de conteúdo, delineando suas atividades e responsabilidades específicas, fornecendo uma base para a compreensão das suas funções e obrigações.

Os provedores de *backbones* são responsáveis pela infraestrutura central da internet, gerenciando as principais redes de transmissão de dados que conectam diferentes regiões e países. Eles mantêm as linhas de alta capacidade que permitem o tráfego de grandes volumes de dados, sendo essenciais para a interconectividade global da rede. Os provedores de acesso, por outro lado, são os que oferecem a conexão direta aos usuários finais, possibilitando que indivíduos e empresas se conectem à internet. Eles são a interface principal entre o usuário e a rede global, tornando sua atuação fundamental para a experiência de navegação dos consumidores.

Além disso, Leonardi identifica os provedores de correio eletrônico, de hospedagem e de conteúdo como categorias com funções distintas e igualmente importantes. Os provedores de correio eletrônico oferecem serviços de e-mail, uma ferramenta vital para a comunicação pessoal e empresarial. Já os provedores de hospedagem disponibilizam espaço em servidores para que indivíduos e empresas possam armazenar e disponibilizar seus sites e dados na internet. Por fim, os provedores de conteúdo são responsáveis pela criação e distribuição de informações, entretenimento e outros materiais acessíveis online. Cada uma dessas categorias de provedores tem

23. Sobre o conceito, explica Victor Auilo Haikal: "Por preciosismo no conceito apresentado, indicar que "a comunicação de dados entre terminais por meio de diferentes redes" não é adequado, pois a rede é uma só: a internet. Ainda que acessada por diversas partes do planeta e sob os mais diferentes números de IP, os *backbones* de cada país se encarregam de realizar a integração da conexão dos terminais aos demais *backbone*s, indiretamente, possibilitando a conexão entre dois *end-points*". HAIKAL, Victor Auilo. Da significação jurídica dos conceitos integrantes do art. 5º. In: LEITE, George Salomão; LEMOS, Ronaldo (coord.). *Marco Civil da Internet*. São Paulo: Atlas, 2014. p. 320.

responsabilidades específicas em relação à segurança, privacidade e gestão dos dados de seus usuários, moldando assim o panorama jurídico e operacional da internet no Brasil.

2. DEVERES DE GUARDA DE REGISTROS E CONTEXTOS ESPECÍFICOS

Antes da promulgação do Marco Civil da Internet, a responsabilidade dos provedores de internet no Brasil era um tema controverso e objeto de disputas judiciais. Algumas decisões judiciais atribuíam responsabilidade aos provedores pelo conteúdo hospedado, o que gerava insegurança jurídica. O Marco Civil da Internet (Lei nº 12.965/2014) define três tipos de agentes responsáveis pela operação da internet no Brasil: provedores de conexão, provedores de aplicação e usuários. A lei estabeleceu, ainda, princípios como a neutralidade da rede, proteção de dados e privacidade, e responsabilidade dos provedores, fornecendo um arcabouço jurídico claro para a operação da internet no país²⁴.

A legislação também estabeleceu obrigações claras de registros de acesso a aplicações e à conexão para esses provedores. Fabio Nori indica quatro categorias de guarda: aquelas necessárias, as vedadas, as autorizadas e as obrigatórias. No contexto da guarda obrigatória, os registros de conexão devem ser mantidos por um ano, enquanto os de acesso a aplicações devem ser mantidos por seis meses. Estas medidas são fundamentais para garantir a segurança e a privacidade dos dados dos usuários, promovendo um ambiente digital mais seguro²⁵. A falta de regulamentação específica contribuía para essa incerteza, criando um ambiente de incerteza jurídica para os provedores, inclusive sobre conceitos técnicos absolutamente importantes, como comenta Marcel Leonardi:

24. LEONARDI, Marcel. A garantia fundamental do direito à privacidade e à liberdade de expressão nas comunicações como condição ao pleno exercício do direito de acesso à internet. In: LEITE, George Salomão; LEMOS, Ronaldo (coord.). *Marco Civil da Internet*. São Paulo: Atlas, 2014. p. 621-633.

25. NORI, Fabio. A guarda dos registros de conexão e dos registros de acesso às aplicações no Marco Civil. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coord.). *Direito & Internet III: Marco Civil da Internet (Lei nº 12.965/2014)*. São Paulo: Quartier Latin, 2015, t. II. p. 169-190.

“Esclareça-se que os dados cadastrais consistem nas informações pessoais fornecidas pelo usuário ao provedor de serviços, tais como nome, endereço, números de documentos pessoais ou empresariais e demais informações necessárias à instalação, funcionamento e cobrança dos serviços. Os dados de conexão consistem nos endereços IP utilizados durante o acesso à Internet, bem como em outras informações relativas ao uso da rede, tais como datas e horários de login e logout, nome de usuário utilizado e demais informações técnicas que tenham por objetivo identificar determinado usuário. Não englobam, portanto, o conteúdo das comunicações nem as transmissões de dados realizadas pelo usuário, mas apenas os dados vinculados à sua identificação ao acessar um serviço on-line”²⁶.

Toda transação na internet gera um registro nos equipamentos, que ficam armazenados por curto período de tempo e passam por análise dos provedores, que verificam se guardarão ou não os dados²⁷. Esse registro é comumente conhecido com “logs de acesso”, e fornecem informações suficientes para se determinar determinado perfil de comportamento online, a partir da navegação na rede virtual. O termo log remonta à navegação, sendo os *log books* os livros de percurso mantido pelo capitão de um navio, que permite verificar por onde a embarcação transitou²⁸.

26. LEONARDI, Marcel. Marco Civil da Internet e proteção de dados pessoais. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coord.). *Direito & Internet III: Marco Civil da Internet* (Lei nº 12.965/2014). São Paulo: Quartier Latin, 2015, t. I. p. 531.

27. Segundo Mário Furlaneto Neto e Bruna Pinotti Garcia: “Define aplicações de internet como “o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet”, ao passo que os registros de acesso a aplicações de internet compreendem o “conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP”. A análise do texto legal permite concluir se tratar do registro inicial de acesso à aplicação de internet, sem fazer menção ao tempo ou duração do acesso ao aplicativo, informação esta eventualmente indispensável para a comprovação de um fato ou circunstância, como o fez ao definir a amplitude do registro de conexão à internet”. FURLANETO NETO, Mário; GARCIA, Bruna Pinotti. Da guarda de registro de acesso a aplicações de internet na provisão de aplicações. In: LEITE, George Salomão; LEMOS, Ronaldo (coord.). *Marco Civil da Internet*. São Paulo: Atlas, 2014. p. 783.

28. NORI, Fabio. A guarda dos registros de conexão e dos registros de acesso às aplicações no Marco Civil. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coord.). *Direito & Internet III: Marco Civil da Internet* (Lei nº 12.965/2014). São Paulo: Quartier Latin,

Guarda, é, portanto, a decisão de se armazenar as informações de acesso por prazo superior ao necessário ao tratamento no equipamento. As regras para guarda dos logs são dispostas no Marco Civil da Internet, que, além de discriminar as hipóteses de armazenamento, também define os limites, a fim de “atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas”. Outro ponto relevante é que esses registros, uma vez armazenados, somente podem ser disponibilizados mediante ordem judicial²⁹. Segundo Fábio Nori³⁰, a guarda dos logs pode ser classificada em quatro tipos de espécies, conforme tabela abaixo.

Tabela 1 - Espécies de guardas de logs

Espécie	Explicação	Fundamento legal
Necessária	Guarda é necessária para controlar o acesso à rede por existência de débito	art. 7º, IV do Marco Civil da Internet ³¹
Vedada	Guarda é vedada em função da necessidade de se	arts. 14 e 16, I do Marco Civil da Internet ³²

2015, t. II. p. 169.

29. “Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas. § 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º”.

30. NORI, Fábio. A guarda dos registros de conexão e dos registros de acesso às aplicações no Marco Civil. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coord.). *Direito & Internet III: Marco Civil da Internet* (Lei nº 12.965/2014). São Paulo: Quartier Latin, 2015, t. II. p. 169-190.

31. “Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: (...) IV - não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização”.

32. “Art. 14. Na provisão de conexão, onerosa ou gratuita, é vedado guardar os registros de acesso a

	proteger a privacidade e os dados pessoais do titular	
Autorizada	Guardas que dependem do consentimento do titular	art. 16, II do Marco Civil da Internet
Obrigatória	Guarda dos registros mandatória pela Lei	art. 13 e 15 do Marco Civil da Internet ³³

Fonte: elaborada pelos autores

Para os propósitos deste artigo, trabalhar-se-á com a espécie obrigatória de registros, analisando os principais tópicos objeto de discussão. Os registros dessa espécie têm, por propósito, permitir a identificação de usuários para viabilizar eventual responsabilização por danos causados a outros usuários. Assim, conforme já havia indicado Marcel Leonardi, ainda em 2005:

“O tempo de manutenção de tais registros é de importância fundamental para a vítima, na medida em que delimita, ainda que indiretamente, verdadeiro prazo decadencial. Esgotado o período de manutenção de tais informações, tornar-se-á praticamente impossível conhecer-se o responsável pelo ato ilícito, impedindo a propositura de ação de reparação de danos e demais”³⁴.

aplicações de internet”; “Art. 16. Na provisão de aplicações de internet, onerosa ou gratuita, é vedada a guarda: I - dos registros de acesso a outras aplicações de internet sem que o titular dos dados tenha consentido previamente, respeitado o disposto no art. 7º ; ou II - de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular, exceto nas hipóteses previstas na Lei que dispõe sobre a proteção de dados pessoais”.

33. “Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento”; “Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento”.

34. LEONARDI, Marcel. *Responsabilidade civil dos provedores de serviços de internet*. São Paulo: Juarez de Oliveira, 2005, p. 55.

Percebe-se, pela leitura dos arts. 5º, VI e VIII, 13 e 15 do Marco Civil da Internet, que os provedores de conexão são obrigados a armazenar, por 1 ano, os registros de conexão, assim entendidos como o conjunto de informações “referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados”. Os provedores de aplicação, por sua vez, são obrigados a armazenar, por 6 meses, os registros de acesso a aplicações de internet, ou seja, “o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP”.

A Convenção de Budapeste, que entrou em vigência no ordenamento jurídico brasileiro a partir do Decreto nº 11.491/2023, fixou, em seu artigo 16, item 1, que as partes que aderirem à Convenção devem adotar as “medidas legislativas e outras providências necessárias para permitir que a autoridade competente ordene ou obtenha a expedita preservação de **dados de computador especificados**, incluindo **dados de tráfego**”. Dado de computador, conforme alínea “b” do artigo 1, é “qualquer representação de fatos, informações ou conceitos numa forma adequada para o processamento num sistema de computador que inclua um programa capaz de fazer o sistema realizar uma tarefa”. Dados de tráfego, por sua vez, conforme alínea “d”, são “quaisquer dados de computador referentes a uma comunicação por meio de um sistema informatizado, gerados por um computador que seja parte na cadeia de comunicação, e que indicam sua origem, destino, caminho, hora, data, extensão, duração ou tipo de serviço subordinado”.

No artigo 16, item 2, a Convenção dispõe sobre as medidas legislativas a serem adotadas pelos Estados para obrigar uma parte a “preservar e manter a integridade desses dados de computador pelo período de tempo necessário, até o máximo de 90 (noventa) dias, a fim de permitir à autoridade competente buscar sua revelação”. Esse prazo, inclusive, poderá ser renovado, caso haja requerimento.

O Marco Civil da Internet deu cumprimento a essa disposição³⁵, obrigando

35. GONÇALVES, Victor Hugo Pereira. *Marco Civil da Internet comentado*. São Paulo: Atlas, 2016. *E-book*. Comenta o autor: “O provedor de acesso à internet fornece uma série de IP (protocolos de internet) válidos (fixos ou dinâmicos), para que o usuário possa se conectar à internet. Assim, o usuário de internet, com o endereço IP atribuído pelo provedor de conexão, conecta-se com os

provedores de conexão a armazenar os registros de conexão por um ano, bem como os provedores de aplicação a armazenar os registros de acesso a aplicações de internet por um ano. Assim, um primeiro ponto de discussão paira sobre as razões técnicas ou jurídicas para se determinar os respectivos prazos de seis meses para provedores de aplicação e um ano para provedores de conexão³⁶.

Um segundo ponto de discussão que se coloca é: os prazos de armazenamento são máximos ou mínimos? Pela leitura conjunta do Marco Civil da Internet e disposições da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), nos parece que o prazo é mínimo. Se houver fundamentação legal para ampliar o armazenamento, seja para o exercício regular de direitos em processos judiciais, seja pelo legítimo interesse do controlador, o provedor de conexão ou aplicação poderá estender esse armazenamento por prazo superior ao fixado pelo Marco Civil da Internet, desde que haja finalidade e base legal para tanto.

Sob o ponto de vista do titular dos dados armazenados, faria sentido uma preservação por tempo superior. Para Marcel Leonardi³⁷, o prazo de três anos seria adequado para a propositura de ações de reparação, à luz do art. 206, § 3º, inciso V do Código Civil³⁸. Para os provedores, contudo, prazo tão longo poderia impor ônus excessivos, ao ser necessário dedicar maior espaço de armazenamento em seus servidores, o que teria um custo adicional.

Em determinadas situações, contudo, os prazos de seis meses, um ano, ou até mesmo três anos, poderiam ser insuficientes para que se busque a devida responsabilização. Por isso, é importante que a parte interessada requeira, na forma do art. 22 do Marco Civil da Internet, a título cautelar, o fornecimento de registros de conexão

provedores de aplicações de internet. O dispositivo de informação e comunicação, com o seu endereço IP já atribuído, conecta-se com os provedores de aplicações de internet desta forma: o IP 177.203.201.21 requer dados do IP 200.173.122.12, que é do sítio fictício <http://www.kant.com.br>”.

36. Este artigo, contudo, não tem como propósito aprofundar essa discussão, pois essas razões técnicas ou jurídicas não são o foco do estudo.

37. LEONARDI, Marcel. *Responsabilidade civil dos provedores de serviços de internet*. São Paulo: Juarez de Oliveira, 2005, p. 55.

38. É importante destacar que este prazo foi proposto em 2005, quase dez anos antes da promulgação do Marco Civil da Internet.

ou de registros de acesso a aplicações de internet, para que estes não se percam. Também é possível requerer o armazenamento por tempo superior. Conforme art. 13 e 15 do Marco Civil da Internet, a autoridade policial ou administrativa ou o Ministério Público poderá requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto no *caput*. Nesse caso, a autoridade requerente terá o prazo de 60 (sessenta) dias, contados a partir do requerimento, para ingressar com o pedido de autorização judicial de acesso aos registros previstos no *caput*.

É possível, ainda que ordem judicial obrigue, por tempo certo, a guarda dos registros de aplicação para os provedores de aplicação que não se enquadrem na categoria do *caput* do art. 15, ou seja, que não sejam constituídos na forma de pessoa jurídica e que não exerçam atividade de forma organizada, profissionalmente e com fins econômicos (art. 15, §1º do Marco Civil da Internet). Neste caso, contudo, os registros devem ser relativos a fatos específicos em período determinado.

Outro ponto de questionamento diz respeito à possibilidade dos provedores de internet deletar os registros após serem citados em processo judicial, se já houver escoado os respectivos prazos de armazenamento. Nesta hipótese, nos parece que, como a citação válida torna litigiosa a coisa (conforme art. 240 do Código de Processo Civil), a destruição dos registros após a citação poderia configurar ato atentatório à dignidade da justiça, por praticar inovação ilegal no estado de fato de bem ou direito litigioso (art. 77, VI, §1º do Código de Processo Civil).

O quarto item dos nossos questionamentos diz respeito à possibilidade de cafés, shoppings e outros estabelecimentos que oferecem internet gratuitamente serem classificados como provedores de conexão. Entendemos que, apesar de fornecer internet, esses estabelecimentos não se amoldam ao art. 13 do Marco Civil da Internet, ou seja, não são considerados como Administradores de Sistema Autônomo (“ASA”). Nos termos do art. 5º, IV do Marco Civil da Internet, o ASA é a pessoa física ou jurídica que administra blocos de IP e o respectivo sistema autônomo de roteamento, sendo cadastrados no ente nacional responsável³⁹. Isso significa que eles

39. As organizações que gerenciam os endereços IP e ASNs são chamadas de NIRs (National Internet Registries) ou Registros Nacionais de Internet. Na América Latina, na região do LACNIC, há dois NIRs: o NIC.br, no Brasil, e o NIC México. Portanto, o NIC.br, por meio do Registro.br, é responsável pela distribuição dos endereços IP e dos ASNs para os provedores de internet brasileiros.

estão dispensados de armazenar os registros de acesso? A resposta a essa pergunta depende do estado onde tais estabelecimentos se encontram. Por exemplo, conforme nos relembra Fábio Nori⁴⁰, a Lei Estadual nº 12.228/2006, do estado de São Paulo, obriga os estabelecimentos comerciais instalados no Estado de São Paulo que ofertam a locação de computadores e máquinas para acesso à internet, utilização de programas e de jogos eletrônicos, tais como “lanhouses”, cibercafés e “cyber offices”, entre outros, a criar e manter cadastros dos usuários, contendo nome, data de nascimento, endereço completo, telefone e número do documento de identidade⁴¹.

Outro ponto de reflexão paira sobre a necessidade de guarda dos *logs* pelos aplicativos que não estão conectados à internet⁴². Isso porque o art. 15 do Marco Civil da Internet obriga os provedores de aplicação de internet a manter os registros de aplicação respectivos, ou seja, os registros de acesso à aplicação, sem conexão com internet, a princípio, não estariam contidos na obrigação legal. Contudo, como grande parte dos aplicativos são baixados (*download*) pela internet, nos parece que o provedor responsável pela hospedagem da aplicação (como Apple Store e Google Play), devem observar a exigência do registro. Ainda, conforme já explicamos, pelo §1º do art. 15 do Marco Civil da Internet, ordem judicial pode obrigar os provedores de aplicação que não se enquadrem no *caput* a armazenar os registros. Assim, em tese, caso haja determinação de um juiz, os provedores de aplicação que não estão conectados à internet poderiam ser obrigados a armazenar os registros pelo prazo de seis meses.

Por fim, um último questionamento: o rol das informações que devem ser armazenadas pelos provedores de internet é exemplificativo ou taxativo? Antes de

40. NORI, Fábio. A guarda dos registros de conexão e dos registros de acesso às aplicações no Marco Civil. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coord.). *Direito & Internet III: Marco Civil da Internet* (Lei nº 12.965/2014). São Paulo: Quartier Latin, 2015, t. II, p. 187.

41. “Artigo 1º - São regidos por esta lei os estabelecimentos comerciais instalados no Estado de São Paulo que ofertam a locação de computadores e máquinas para acesso à internet, utilização de programas e de jogos eletrônicos, abrangendo os designados como “lanhouses”, cibercafés e “cyber offices”, entre outros”; “Artigo 2º - Os estabelecimentos de que trata esta lei ficam obrigados a criar e manter cadastro atualizado de seus usuários, contendo: I - nome completo; II - data de nascimento; III - endereço completo; IV - telefone; V - número de documento de identidade”.

42. Como exemplo, podemos citar jogos como Minecraft, Pokémon Quest, Fruit Ninja e Polytopia.

adentrarmos na resposta, vamos aprofundar no conceito de IP (*Internet Protocol*) e portas lógicas.

3. ENDEREÇO IP E PORTAS LÓGICAS

3.1. *Internet Protocol* (IP)

Conforme ensina Andrew Tanenbaum, “na Internet, cada *host* e cada roteador tem um endereço IP que codifica seu número de rede e seu número de host, sendo essa combinação exclusiva. Em tese, duas máquinas não possuem o mesmo endereço”⁴³. O IP identifica seus destinatários e remetentes a partir do conjunto de quatro números de até três dígitos que permitem que pacotes de dados sejam transmitidos entre terminais conectados a uma rede. Cada hardware conectado à internet, os servidores que hospedam um site, possui um endereço de IP único⁴⁴. Contudo, lembrar tais endereços não é fácil, e, por isso, eles são traduzidos para o sistema DNS (*Domain Network System*)⁴⁵, infraestrutura que permite que usuários entrem em sites todos os dias (por exemplo, acessando o Google por meio do endereço *www.google.com.br*). Esse conjunto de letras corresponde ao conjunto de números do IP.

A versão mais utilizada atualmente é a quarta versão deste protocolo, ou seja, o IPv4, utilizada amplamente pela internet comercial desde seu início, na década de 1990⁴⁶. Como esta versão conta com um total de 4,3 bilhões de endereços⁴⁷,

43. TANENBAUM, Andrew S. *Computer Networks*. 4. ed. Rio de Janeiro: Pearson Prentice Hall, 2011, p. 334.

44. FROSIO, Giancarlo. Mapping Online Intermediary Liability. In: FROSIO, Giancarlo (ed.). *The Oxford Handbook of Online Intermediary Liability*. Oxford: Oxford University Press, 2020, p. 633-634.

45. FROSIO, Giancarlo. Mapping Online Intermediary Liability. In: FROSIO, Giancarlo (ed.). *The Oxford Handbook of Online Intermediary Liability*. Oxford: Oxford University Press, 2020, p. 633-634..

46. INSTITUTO DE REFERÊNCIA EM INTERNET E SOCIEDADE - IRIS. Portas Lógicas e Registros de Acesso: das possibilidades técnicas aos entendimentos dos tribunais brasileiros. 2017, p. 5.

47. Comenta a doutrina: “Os provedores de conexão à internet têm disponíveis um determinado número de IPs (“blocos de endereço IP”) para que seus clientes utilizem. Porém, como não há IPs suficientes a todos os usuários da rede e nem todos eles acessam a rede ao mesmo tempo, o provedor de conexão faz uma espécie de “rodízio” de IPs. Simplificadamente, cada vez que o usuário

atualmente não há mais novos endereços disponíveis, sendo necessário implementar uma outra versão do protocolo, o IPv6. Esta versão, que utiliza quatro dígitos hexadecimais, conta com um total de 3.4×10^{38} endereços (mais que o total estimado de estrelas no universo conhecido)⁴⁸, e será suficiente para distribuir endereços pelas próximas décadas⁴⁹.

3.2. Portas lógicas

O esgotamento do IPV4 levou à necessidade de compartilhamento dos endereços por meio do sistema NAT (*Network Address Translation*), que permite que vários dispositivos em uma rede de IPs privados compartilhem um único IP público quando desejarem se conectar a uma rede externa, a internet⁵⁰. Dessa forma,

acessa a rede, um IP de numeração diferente é designado ao seu terminal. Ao se desconectar da rede, aquele IP é designado a outro terminal e assim sucessivamente. Esse roteamento de IPs é automático e necessário para que todos possam acessar a rede, em um ambiente de IPs limitados”. KUJAWSKI, Fábio Ferreira; THOMAZ, Alan Campos Elias. Da proteção aos registros, dados pessoais e comunicações privadas - um enfoque sobre o Marco Civil da Internet. In: LEITE, George Salomão; LEMOS, Ronaldo (coord.). *Marco Civil da Internet*. São Paulo: Atlas, 2014. p. 687.

48. INSTITUTO DE REFERÊNCIA EM INTERNET E SOCIEDADE - IRIS. Portas Lógicas e Registros de Acesso: das possibilidades técnicas aos entendimentos dos tribunais brasileiros. 2017, p. 5.

49. MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti; FALEIROS JÚNIOR, José Luiz de Moura. Porta lógica, IP e os registros de acesso a aplicações da Internet: uma leitura ampliada do art. 5º, VIII, do Marco Civil da Internet. *Jota*, 26 dez. 2019. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/porta-logica-ip-e-os-registros-de-acesso-a-aplicacoes-da-internet-26122019> Acesso em: 30 maio 2024.

50. Em relação ao tema, “[q]uando o usuário faz a conexão ao provedor de aplicação de internet, a informação armazenada pelo provedor de aplicação será a do IP atribuído pelo provedor de conexão contratado pelo estabelecimento que fornece a rede sem fio e que, ao ser instado, revelará ter atribuído o IP ao estabelecimento que funciona, na prática, como roteador, não sendo possível, portanto, identificar qual dentre os usuários finais fez uso do IP na data e horário investigados, justamente por ausência de armazenamento de tais informações. O legislador infraconstitucional deveria ter ido além para, também, estabelecer a obrigatoriedade de manutenção dos registros de acesso às pessoas jurídicas que redistribuem o sinal de internet, enquanto intermediárias do provedor de acesso”. FURLANETO NETO, Mário; GARCIA, Bruna Pinotti. Da guarda de registro de acesso a aplicações de internet na provisão de aplicações. In: LEITE, George Salomão; LEMOS, Ronaldo (coord.). *Marco Civil da Internet*. São Paulo: Atlas, 2014. p. 784.

conforme o Instituto de Referência em Internet e Sociedade (IRIS), “o sistema de NAT direciona os pacotes de dados entrando e saindo através dele, utilizando-se de portas que o permitem identificar qual dispositivo se conecta com qual endereço externo. As portas são um número acrescentado ao final do endereço de IP, que permitem ao NAT criar uma tabela de associações e viabilizar sua função”⁵¹. A tabela abaixo ilustra essa associação.

Tabela 2 - Exemplo de tabela de vinculação de endereços

IP Privado	IP Público/Global
192.168.1.103:3663	152.238.154.3:3663
192.168.1.101:4554	152.238.154.3:4554
192.168.1.105:2882	152.238.154.3:2882

Fonte: IRIS, 2017.

De posse dessas informações, pode-se retomar a pergunta feita ao final do capítulo anterior: o rol das informações que devem ser armazenadas pelos provedores de internet é exemplificativo ou taxativo?

O Superior Tribunal de Justiça (STJ), no julgamento do Recurso Especial (REsp) nº 1.784.156/SP, de relatoria do Ministro Marco Aurélio Bellizze, definiu que os endereços de IP são os dados essenciais para identificação do dispositivo utilizado, e, como há a necessidade de compartilhar os IPs, a individualização da navegação na internet passa a depender da porta lógica de origem, até a migração para o IPv6:

RECURSO ESPECIAL. CIVIL E PROCESSUAL CIVIL. AÇÃO DE OBRIGAÇÃO DE FAZER. PROVEDOR DE APLICAÇÕES. IDENTIFICAÇÃO DO DISPOSITIVO UTILIZADO PARA ACESSO À APLICAÇÃO. INDICAÇÃO DO ENDEREÇO IP E PORTA LÓGICA DE ORIGEM. INTERPRETAÇÃO TELEOLÓGICA DOS ARTS. 5º, VII, E 15 DA LEI N. 12.965/2014. RECURSO ESPECIAL PROVIDO.

(...) 2. A previsão legal de guarda e fornecimento dos dados de acesso de conexão e aplicações foi distribuída pela Lei n. 12.965/2014 entre os

51. INSTITUTO DE REFERÊNCIA EM INTERNET E SOCIEDADE - IRIS. Portas Lógicas e Registros de Acesso: das possibilidades técnicas aos entendimentos dos tribunais brasileiros. 2017, p. 6.

provedores de conexão e os provedores de aplicações, em observância aos direitos à intimidade e à privacidade.

3. Cabe aos provedores de aplicações a manutenção dos registros dos dados de acesso à aplicação, entre os quais se inclui o endereço IP, nos termos dos arts. 15 combinado com o art. 5º, VIII, da Lei n. 12.965/2014, os quais poderão vir a ser fornecidos por meio de ordem judicial.

4. A obrigatoriedade de fornecimento dos dados de acesso decorre da necessidade de balanceamento entre o direito à privacidade e o direito de terceiros, cujas esferas jurídicas tenham sido aviltadas, à identificação do autor da conduta ilícita.

5. Os endereços de IP são os dados essenciais para identificação do dispositivo utilizado para acesso à internet e às aplicações.

6. A versão 4 dos IPs (IPv4), em razão da expansão e do crescimento da internet, esgotou sua capacidade de utilização individualizada e se encontra em fase de transição para a versão 6 (IPv6), fase esta em que foi admitido o compartilhamento dos endereços IPv4 como solução temporária.

7. Nessa fase de compartilhamento do IP, a individualização da navegação na internet passa a ser intrinsecamente dependente da porta lógica de origem, até a migração para o IPv6.

8. A revelação das portas lógicas de origem consubstancia simples desdobramento lógico do pedido de identificação do usuário por IP.

9. Recurso especial provido⁵².

Como dito anteriormente, a guarda dos registros exigidos pelo Marco Civil da Internet tem como propósito individualizar as condutas na internet para fins de responsabilização. E, inegavelmente, a chamada porta lógica (*logicalchannel*, *virtual channel*, *virtual circuit* etc.) permite saber com exatidão qual é o terminal conectado a um IP que esteja sendo compartilhado em determinado momento⁵³.

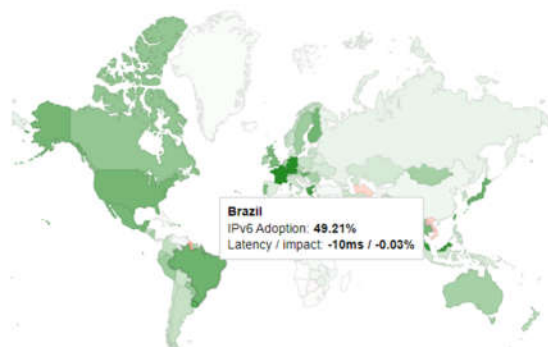
52. BRASIL. Superior Tribunal de Justiça. *Recurso Especial n. 1.784.156/SP*. Relator Ministro Marco Aurélio Bellizze, Terceira Turma, julgado em 5 nov. 2019, Diário da Justiça Eletrônico, 21 nov. 2019.

53. Diz a doutrina: “None of the physical connections between nodes (i.e., links) in a packet-switched

Portanto, caso futuramente haja a necessidade de se fornecer outras informações para tal finalidade, entendemos que o julgando do STJ permite a interpretação de que o rol do art. 13 e 15 do Marco Civil da Internet seria exemplificativo, podendo os provedores de internet serem obrigados a armazenar outras informações para além daquelas constantes na Lei. Contudo, em nome da segurança jurídica, entendemos que a obrigação somente poderia ser imputada aos provedores através de decisão judicial, e mediante razoável justificativa pela parte interessada.

Por fim, a obrigação de guarda da porta lógica cabe tanto aos provedores de conexão quanto aos de aplicação. Segundo o STJ no julgando do REsp nº 2.005.051/SP, de relatoria da Ministra Nancy Andrighi, “da interpretação sistemática de dispositivos legais do Marco Civil da Internet (art. 10, caput e § 1º, e art. 15), deduz-se que tanto os provedores de conexão quanto os provedores de aplicação têm a obrigação de guarda e fornecimento das informações da porta lógica de origem associada ao endereço IP”. Isso porque, segundo a ministra, “apenas com as duas pontas da informação - conexão e aplicação - é possível resolver a questão da identidade de usuários na internet que estejam utilizando um compartilhamento da versão 4 do IP”.

Figura 1 - Nível de adoção do IPV6 por país



Fonte: Google

network are dedicated to the carriage of any single message. Instead, the use of the links is shared. The individual packets of a single message are jumbled up with packets from other messages. For the end-users, however, the effect is nonetheless as if a ‘permanent’ channel existed between the two ends (as shown in Figure 2.23).⁵ Each ‘channel’ is known as a logical channel, virtual channel or virtual circuit.” CLARK, Martin P. *Data networks, IP and the Internet: protocols, design and operation*. West Sussex: WileyEurope, 2003. p. 58.

Apesar da obrigatoriedade da guarda de vários registros, parte das obrigações definidas por meio da construção jurisprudencial do STJ deve ser alterada nos próximos. Com a implementação do IPV6, a tendência é que a necessidade de armazenamento da porta lógica pelos provedores de conexão e aplicação se torne obsoleta. O gráfico abaixo, retirado do Google, mostra o nível de adoção de IPV6 por cada país⁵⁴.

Apesar desta provável simplificação futura, conforme defendido neste trabalho, alertamos para o fato de que, futuramente, a guarda de outras informações pode ser exigida face à necessidade de se individualizar as condutas em ambiente *online* e permitir a responsabilização por danos causados. É importante, de igual maneira, estar atento à evolução legislativa sobre o tema, em especial considerando a reforma pretendida do Código Civil, a introdução do livro de Direito Digital, e os impactos que tais mudanças podem ter nos provedores de internet.

CONCLUSÃO

Este artigo detalhou a evolução e o impacto do Marco Civil da Internet na categorização e nas responsabilidades dos provedores de internet no Brasil. Vimos que, antes de sua promulgação, a ausência de regulamentação específica criava uma insegurança jurídica que afetava tanto os provedores de telecomunicações quanto os provedores de aplicação de internet, resultando em decisões judiciais muitas vezes contraditórias. Exploramos as diversas propostas teóricas de categorização dos provedores de internet, comparando-as com a realidade jurídica brasileira. As contribuições teóricas de autores como Lawrence Lessig, Pedro de Miguel Asensio, Tim Wu e Marcel Leonardi foram fundamentais para contextualizar as funções e responsabilidades dos provedores dentro do ecossistema digital.

Com o Marco Civil da Internet, uma nova estrutura regulatória foi estabelecida, trazendo clareza e segurança jurídica ao definir princípios como a neutralidade da rede, a proteção de dados e a privacidade. Ainda, a lei categorizou os provedores de internet entre provedores de conexão e aplicação, definindo suas responsabilidades. Dentre as responsabilidades, destacamos aquelas referentes à guarda dos registros de

54. Note-se que os níveis foram avaliados à época de escrita deste artigo, em maio de 2024. É possível que, durante a leitura por você, leitor, estes níveis estejam mais avançados.

conexão e acesso às aplicações, bem como enfrentamos os principais tópicos de debate sobre esses registros.

A não observância dessas obrigações pelos provedores de internet podem ter implicações profundas nos modelos de negócios desses agentes. Podemos destacar, pelo Marco Civil da Internet, e para a inobservância do dever de guarda ou fornecimentos dos registros pelos provedores de internet, sanções como advertência, multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, à suspensão temporária das atividades que envolvam os atos previstos no art. 11 e proibição de exercício das atividades que envolvam os atos previstos no art. 11. Neste último cenário, a sanção poderia implicar em proibição total das atividades dos provedores, impactando de forma substancial a atividade econômica do agente. Para além disso, a inobservância dos deveres quanto à preservação dos dados pessoais e da privacidade dos titulares pode atrair, também, a incidência e as sanções previstas na LGPD.

REFERÊNCIAS

- BRASIL. Decreto nº 11.491, de 12 de abril de 2023. *Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste*. Diário Oficial da União: seção 1, Brasília, DF, 13 abr. 2023.
- BRASIL. Lei nº 12.965, de 23 de abril de 2014. *Marco Civil da Internet*. Diário Oficial da União, Brasília, DF, 24 abr. 2014.
- BRASIL. Lei nº 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados Pessoais*. Diário Oficial da União, Brasília, DF, 15 ago. 2018.
- BRASIL. Lei nº 9.472, de 16 de julho de 1997. *Dispõe sobre a organização dos serviços de telecomunicações*. Diário Oficial da União, Brasília, DF, 17 jul. 1997.
- BRASIL. Superior Tribunal de Justiça. *Recurso Especial 1.784.156/SP*. Relator: Min. Ricardo Villas Bôas Cueva. Julgado em 14/08/2019. Diário da Justiça Eletrônico, 21/11/2019.
- BRASIL. Superior Tribunal de Justiça. *Recurso Especial 2.005.051/SP*. Relator: Min. Paulo de Tarso Sanseverino. Julgado em 10/03/2023. Diário da Justiça Eletrônico, 25/8/2022.
- BRASIL. Superior Tribunal de Justiça. *Recurso Especial 997.993/MG*. Relator: Ministro Luis Felipe Salomão. Julgado em 21/06/2012. Diário da Justiça Eletrônico, 06/08/2012.
- CLARK, Martin P. *Data networks, IP and the Internet: protocols, design and operation*. West Sussex: WileyEurope, 2003.

- DE LUCCA, Newton. Marco Civil da Internet - uma visão panorâmica dos principais aspectos relativos às suas disposições preliminares. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coord.). *Direito & Internet III: Marco Civil da Internet* (Lei nº 12.965/2014). São Paulo: Quartier Latin, 2015, t. I.
- DE MIGUEL ASENSIO, Pedro A. *Derecho Privado de Internet*. 6. ed. Cizur Menor (Navarra): Civitas, 2022.
- ESTADOS UNIDOS DA AMÉRICA. *Digital Millennium Copyright Act (DMCA)*. Public Law 105-304, 1998. Disponível em: <https://www.copyright.gov/legislation/dmca.pdf> Acesso em: 14 maio 2024.
- FROSIO, Giancarlo. Mapping Online Intermediary Liability. In: FROSIO, Giancarlo (ed.). *The Oxford Handbook of Online Intermediary Liability*. Oxford: Oxford University Press, 2020.
- FURLANETO NETO, Mário; GARCIA, Bruna Pinotti. Da guarda de registro de acesso a aplicações de internet na provisão de aplicações. In: LEITE, George Salomão; LEMOS, Ronaldo (coord.). *Marco Civil da Internet*. São Paulo: Atlas, 2014. p. 772-790.
- GETSCHKO, Demi. As origens do Marco Civil da Internet. In: LEITE, George Salomão; LEMOS, Ronaldo (coord.). *Marco Civil da Internet*. São Paulo: Atlas, 2014. p. 12-17.
- GONÇALVES, Victor Hugo Pereira. *Marco Civil da Internet comentado*. São Paulo: Atlas, 2016. *E-book*.
- HAIKAL, Victor Auilo. Da significação jurídica dos conceitos integrantes do art. 5º. In: LEITE, George Salomão; LEMOS, Ronaldo (coord.). *Marco Civil da Internet*. São Paulo: Atlas, 2014. p. 317-324.
- HERRERÍAS CASTRO, Laura. ¿Matar al mensajero? La responsabilidad de las redes sociales y los usuarios por difamación. *Revista d'Internet, Dret i Política*, Barcelona: Universitat Oberta de Catalunya, n. 40, p. 1-12, mar. 2024.
- INSTITUTO DE REFERÊNCIA EM INTERNET E SOCIEDADE - IRIS. *Portas Lógicas e Registros de Acesso: das possibilidades técnicas aos entendimentos dos tribunais brasileiros*. 2017.
- KUJAWSKI, Fábio Ferreira; THOMAZ, Alan Campos Elias. Da proteção aos registros, dados pessoais e comunicações privadas - um enfoque sobre o Marco Civil da Internet. In: LEITE, George Salomão; LEMOS, Ronaldo (coord.). *Marco Civil da Internet*. São Paulo: Atlas, 2014. p. 677-694.
- LEONARDI, Marcel. A garantia fundamental do direito à privacidade e à liberdade de expressão nas comunicações como condição ao pleno exercício do direito de acesso à internet. In: LEITE, George Salomão; LEMOS, Ronaldo (coord.). *Marco Civil da Internet*. São Paulo: Atlas, 2014. p. 621-633.
- LEONARDI, Marcel. Marco Civil da Internet e proteção de dados pessoais. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coord.). *Direito & Internet III: Marco Civil da Internet* (Lei nº 12.965/2014). São Paulo: Quartier Latin, 2015, t. I. p. 517-538.

- LEONARDI, Marcel. *Responsabilidade civil dos provedores de serviços de internet*. São Paulo: Juarez de Oliveira, 2005.
- LESSIG, Lawrence. *Code and Other Laws of Cyberspace*. 2. ed. Nova York: Basic Books, 2006.
- MARTINS, Guilherme Magalhães. *Responsabilidade Civil por Acidente de Consumo na Internet*. 3. ed. São Paulo: Thomson Reuters Brasil, 2020.
- MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti; FALEIROS JÚNIOR, José Luiz de Moura. Porta lógica, IP e os registros de acesso a aplicações da Internet: uma leitura ampliada do art. 5º, VIII, do Marco Civil da Internet. *Jota*, 26 dez. 2019. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/porta-logica-ip-e-os-registros-de-acesso-a-aplicacoes-da-internet-26122019> Acesso em: 30 maio 2024.
- NORI, Fabio. A guarda dos registros de conexão e dos registros de acesso às aplicações no Marco Civil. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coord.). *Direito & Internet III: Marco Civil da Internet (Lei nº 12.965/2014)*. São Paulo: Quartier Latin, 2015, t. II. p. 169-190.
- QUEIROZ, Renata Capriolli Zocatelli; BENICIO, Mariane Menezes; LATTANZIO, Daniel Zonzini. A não incidência do ISS e do ICMS sobre o serviço de valor adicionado. *Revista Foco*, Curitiba, v. 16, n. 2, p. 1-13, 2023.
- SIMÃO FILHO, Adalberto. Do contrato de concessão para serviços de telecomunicações à telefonia IP-VoIP: reflexos nos direitos transindividuais. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto (coord.). *Direito & Internet II: aspectos jurídicos relevantes*. São Paulo, 2008. p. 77-116.
- TANENBAUM, Andrew S. *Computer Networks*. 4. ed. Rio de Janeiro: Pearson Prentice Hall, 2011.
- TOMASEVICIUS FILHO, Eduardo. O Marco Civil da Internet e as liberdades de mercado. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coord.). *Direito & Internet III: Marco Civil da Internet (Lei nº 12.965/2014)*. São Paulo: Quartier Latin, 2015, t. II. p. 49-64.
- UNIÃO EUROPEIA. *Regulamento (UE) 2022/2065 do Parlamento Europeu e do Conselho de 19 de outubro de 2022 relativo a um Mercado Único de Serviços Digitais e que altera a Diretiva 2000/31/CE (Digital Services Act)*. 2022. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32022R2065> Acesso em: 30 maio. 2024.
- WU, Tim. *The Master Switch: The Rise and Fall of Information Empires*. Nova York: Vintage, 2010.

PROVEDORES DE APLICAÇÃO E CONTEÚDO DE TERCEIROS: UMA ANÁLISE DA EVOLUÇÃO JURISPRUDENCIAL¹

Henrique Almeida Bazan

Mestre e bacharel em Direito pela Universidade Federal de Minas Gerais

DOI: <https://doi.org/10.59224/dti7.ch7>

Resumo: A presente pesquisa almejou analisar e extrair informações a partir de breve recuperação da evolução jurisprudencial em casos correlatos a responsabilidade civil de provedores de aplicação por conteúdos de terceiros. Para fundamentar a pesquisa, foi feita análise jurisprudencial de decisões colhidas no Superior Tribunal de Justiça, em que houve certo desencontro entre a norma do artigo 19 do Marco Civil da Internet e a decisão judicial, haja vista a dificuldade de aplicação do dispositivo diante do modelo de negócio do provedor de aplicação. Foi uma hipótese comprovada na pesquisa que o termo “provedores de aplicação” abrange muitas formas de serviços e que, em casos específicos, tribunais tiveram de decidir de forma diferente ao determinado no Marco Civil da Internet, para conformar a decisão a direitos fundamentais e ao modelo de negócio das aplicações. Concluiu-se que, ainda que o Marco Civil da Internet seja norma de grande importância na busca da homogeneização das decisões em litígios online, é natural que alguns pontos sejam aperfeiçoados após dez anos de sua promulgação. O regime de responsabilidade civil previsto no artigo 19 é de grande valor para preservação do modelo de negócio de provedores de rede social, no entanto não parece ser suficiente para abranger todos os provedores de aplicações.

Abstract: The present research aimed to analyze and extract information from a brief review of the evolution of jurisprudence in matters related to the civil liability of application providers for third-party content. To support the research, a jurisprudence analysis was conducted based on decisions from the Superior Court of Justice, where discrepancies were observed between Article 19 of the Brazilian Internet Bill of Rights (Marco Civil da Internet) and judicial rulings, given the challenges in applying the norm to the business model of the internet intermediary. The research confirmed the hypothesis that the term “application providers” encompasses various types of services and that, in specific cases, courts have had to rule differently from what is prescribed in the Internet Bill of Rights to align decisions with fundamental rights and the business models of applications. It was concluded that, while the Brazilian Internet Bill of Rights is a highly significant regulation for standardizing decisions in online disputes, it is natural that certain aspects require refinement after ten years of its enactment. The civil liability framework established in Article 19 is highly valuable for preserving the business model of social network providers; however, it does not appear to be sufficient to cover all types of application providers.

1. Este artigo foi escrito em maio de 2024, antes, portanto, do julgamento do Tema 987 pelo STF.

Palavras-chave: artigo 19; responsabilidade civil; provedores de aplicação.

Keywords: Article 19; civil liability; internet intermediary.

SUMÁRIO: Introdução; 1. O que são provedores de aplicação; 2. O regime de responsabilidade civil de provedores de aplicação por conteúdos de terceiros; 3. Decisões singulares e a evolução jurisprudencial; 3.1 Provedores de pesquisa; 3.2 Provedores de mensageria criptografados; 3.3 Proteção da criança e do adolescente; 4 Considerações finais; Referências.

INTRODUÇÃO

O papel de centralidade assumida pela internet na vida contemporânea é de difícil dimensionamento, mesmo a partir de dados. A pesquisa TIC Domicílios de 2022² provê exemplos de sua relevância. No período de um ano, entre usuários brasileiros da rede³: 82% utilizou ferramentas de governo eletrônico na internet (para agendamento de consultas, acesso a direitos trabalhistas e outros), 50% comprou algum produto ou serviço, 92% enviou mensagens instantâneas, 80% usou redes sociais, 80% fez chamadas de voz ou vídeo e 88% realizou alguma atividade cultural por intermédio da internet.

Os dados supramencionados retratam parte do uso da internet por brasileiros, o que pode levar a interpretações equivocadas do grau de conectividade existente no país⁴. Ainda que porcentagem altas, um único uso pelo usuário para a finalidade levantada já é suficiente para que ele seja integrado ao grupo dos que fizeram a ação no período de um ano, o que pode mascarar a exclusão digital existente no Brasil. No entanto, é evidente que a internet se tornou instrumento de importância ímpar aos

-
2. Núcleo de Informação e Coordenação do Ponto BR. (2023). *Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros*: pesquisa TIC Domicílios, ano 2022. Disponível em: <https://cetic.br/pt/arquivos/domicilios/2022/domicilios/>
 3. De acordo com a pesquisa, 88% dos brasileiros se consideram usuários de internet.
 4. O percentil de usuário de internet no Brasil não qualifica as condições de acesso do usuário. Em pesquisa do Núcleo de Informação e Coordenação do Ponto BR, identificou-se que apenas 26% da população brasileira alcança níveis considerados adequados de conectividade significativa.

cidadãos, já que facilita demandas cotidianas, conecta-os entre si e permite a oferta de diversas funcionalidades. Os agentes que ofertam serviços na internet disputam usuários em um macro modelo de negócio denominado economia da atenção⁵ e são identificados no ordenamento jurídico brasileiro enquanto “provedores de aplicação”.

A presente pesquisa almeja analisar e extrair informações a partir de breve recuperação da evolução jurisprudencial em casos correlatos a responsabilidade civil de provedores de aplicação por conteúdos de terceiros. Acredita-se que o termo “provedores de aplicação” abrange muitas formas de serviços e que, em casos específicos, tribunais tiveram de decidir de forma diferente ao determinado no Marco Civil da Internet, para conformar a decisão a direitos fundamentais e ao modelo de negócio das aplicações. Na pesquisa, busca-se responder se é possível que todos os provedores de aplicação recebam igual tratamento jurídico quanto ao regime de responsabilidade civil por conteúdos de terceiros.

Haja vista o debate observado globalmente para ampliação da regulação de redes sociais, assim como a observância de atos ilícitos praticados contínua e impunemente na internet brasileira, acredita-se que a adoção do termo “provedores de aplicação” no Marco Civil da Internet⁶ (MCI) não se mostra o caminho mais adequado para regular a responsabilidade civil destes agentes por conteúdos de terceiros. Diante da diversidade de serviços que prestam e cujos impactos sociais são distintos, não parece adequado impor a todos o mesmo regime de responsabilidade civil.

A metodologia utilizada para a condução da pesquisa consistiu em consulta bibliográfica e jurisprudencial para conceituação do termo provedores de aplicação e para discorrer quanto ao regime de responsabilidade civil que lhes foi atribuído no Marco Civil da Internet. No último tópico, foram analisadas decisões judiciais, de modo a extrair informações sobre modelos de negócios de provedores de aplicação e a responsabilidade civil que lhes foi atribuída, além de observar a evolução

5. BENTES, Ana. *A gestão algorítmica da atenção: Enganchar, Conhecer e Persuadir*. In: Seminário Governança das Redes, 4., 2019, Belo Horizonte. Políticas, Internet e Sociedade. Belo Horizonte: IRIS. p. 222-234.

6. BRASIL, Marco Civil da Internet (2014). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 10 de mai. 2024.

jurisprudencial do tema.

O presente trabalho está dividido em quatro partes, além desta introdução. O primeiro tópico apresenta o conceito de “provedores de aplicação”. O segundo discorre quanto ao regime de responsabilidade civil atribuído aos intermediários nos artigos 19 e 21 do Marco Civil da Internet. O terceiro aborda e analisa decisões judiciais em casos sobre provedores de aplicação e conteúdos de terceiros, sendo seguido por considerações finais, em que se pretende discutir os resultados alcançados na pesquisa.

1. O CONCEITO DE PROVEDORES DE APLICAÇÃO

Classificar e agrupar serviços prestados na internet é tema de debate da doutrina jurídica desde o início do século XXI. Com a massificação do uso da internet, verificou-se a transposição de fenômenos sociais antes observados fisicamente para o ciberespaço e, com isso, a necessidade de novas regras para reger tais relações⁷. O debate para classificação desses serviços antecedeu o Marco Civil da Internet, o influenciou e ainda é privilegiado por parte dos magistrados brasileiros em detrimento dos termos consolidados na lei. Entre autores brasileiros, verifica-se que Marcel Leonardi, em sua obra *Responsabilidade Civil dos Provedores de Serviços de Internet*⁸, foi um dos precursores da discussão, que teve solução parcial com a dicotomia estabelecida no Marco Civil da Internet entre provedores de aplicação e provedores de conexão.

O termo “provedor de aplicações de internet” é utilizado no Marco Civil sete vezes e seu plural aparece mais duas vezes na legislação. Ainda que central para a interpretação da lei, ele não é definido, ao menos de forma direta. No artigo 5º, inciso VIII, da lei foi conceituado “aplicações de internet” que consistem em “conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet”. A definição do termo passa, portanto, pela atividade que um agente provê dentro do campo conceituado⁹.

7. CASTELLS, Manuel. *A Galáxia Internet: reflexões sobre a Internet, negócios e a sociedade*. Zahar, 2003.

8. LEONARDI, Marcel. *Responsabilidade civil dos provedores de serviços de internet*. Editora Juarez de Oliveira, 2005.

9. FERNANDES, André (s.d.). Disponível em: <https://ip.rec.br/blog/provedores-de-conteudo-e->

O artigo 15 da lei permite a interpretação de “quem” seria o provedor da atividade com tais características. O dispositivo trata de obrigações ao “provedor de aplicações constituído na forma de pessoa jurídica” e que exerce a “atividade de forma organizada, profissionalmente e com fins econômicos”. Em sequência, o § 1º prevê que outros provedores de aplicação, isto é, que não tenham tais características estruturais mencionadas no caput do dispositivo, também estão sujeitos à obrigação prevista no artigo mediante ordem judicial. Portanto, o legislador optou por não restringir a quem o conceito abarca, inexistindo limitação de natureza jurídica, motivação econômica do agente ou grau de profissionalismo da atividade econômica para sua qualificação enquanto provedor de aplicação.

Dessa forma, depreende-se que provedor de aplicação pode ser pessoa física ou jurídica, que independe de motivação econômica na funcionalidade que oferta na internet para ser compreendido no conceito. A amplitude do conceito, principalmente quanto à natureza jurídica do provedor de aplicação, é importante para confirmar que pessoas físicas, como autores de blogs, são provedores de aplicação, assim como entidades sem fins lucrativos, como a enciclopédia virtual Wikipédia, também estão sujeitas aos dispositivos do Marco Civil da Internet que regulam provedores de aplicação¹⁰.

É possível também extrair mais informações quanto ao que são provedores de aplicação a partir do que o conceito não abarca. Em classificação dicotômica, o MCI conceituou no art. 5º, inciso V, “conexão à internet”, termo já mais difundido em sociedade. Na lei, há o termo “provedor de conexão à internet”, que seria aquele que provê o objeto definido no artigo 5º, V. Em termos práticos, são provedores de conexão à internet as empresas que ofertam acesso à rede. No Brasil, preponderam três grandes provedores e diversos pequenos provedores de conexão em cidades interiores. Os provedores de conexão são condição *sine qua non* para o acesso à internet pelos cidadãos. Tendo em vista que o Marco Civil da Internet impõe obrigações e responsabilidades distintas a provedores de aplicações e de conexão, um conceito atua de forma complementar para compreensão do outro.

aplicacao-interpretacao-do-marco-civil-da-internet/. Acesso em: 10 de mai. 2024.

10. CEROY, Frederico Meinberg. Os conceitos de provedores no Marco Civil da Internet. *Revista Eletrônica Direito & TI*, v. 1, n. 1, p. 3-3, 2015.

Provedores de aplicação são obrigados a guardar registros de acesso dos usuários às aplicações que ofertam por seis meses (art. 15), prazo que pode ser expandido conforme o caso, já que é curto ao se considerar o tempo médio de duração de processos judiciais no Brasil. Já o provedor de conexão não deve guardar registros de acesso de usuários a provedores de aplicação. O regime de responsabilidade civil por conteúdos de terceiros também os difere, pois o primeiro é responsável civilmente caso descumpra uma ordem judicial de indisponibilização de conteúdo, enquanto o segundo, em nenhuma hipótese, será responsabilizado por conteúdos de terceiros. Dessa forma, apenas os provedores de aplicação estão sujeitos à imputação de consequências por conteúdos de terceiros. Conforme se verá adiante, o dispositivo possui outras nuances interpretativas.

Ao se analisar jurisprudências sobre o tema “provedores de aplicação” não se verifica apenas o uso da classificação dicotômica prevista no Marco Civil da Internet, o que ilustra, ao menos em alguma medida, problemas de magistrados brasileiros na compreensão e uso do Marco Civil da Internet. É frequente a menção em acórdãos do Superior Tribunal de Justiça (STJ) a “provedores de pesquisa¹¹”, “provedores de serviços na internet¹²”, “provedores de conteúdo¹³” e outros. O último termo, inclusive, é uma das cinco categorias proposta na classificação de Marcel Leonardi¹⁴. Tais prestadores de serviços na internet aglomerados nos agrupamentos mencionados estão contidos no grande grupo “provedores de aplicação”, ainda que as decisões não mencionam o termo do Marco Civil da Internet.

11. Julgados: REsp 2012895/SP, Rel. Ministra NANCY ANDRIGHI, TERCEIRA TURMA, julgado em 08/08/2023, DJe 15/08/2023; REsp 1937989/SP, Rel. Ministro LUIS FELIPE SALOMÃO, QUARTA TURMA, julgado em 23/08/2022, DJe 07/11/2022; AgInt no AREsp 1085447/SP, Rel. Ministro RAUL ARAÚJO, QUARTA TURMA, julgado em 17/10/2022, DJe 21/10/2022 REsp 2006420/RJ (decisão monocrática), Rel. Ministra MARIA ISABEL GALLOTTI, QUARTA TURMA, julgado em 27/02/2023, publicado em 02/03/2023.

12. Julgado: AgRg no RMS n. 65.270/MT, relatora Ministra Laurita Vaz, Sexta Turma, julgado em 15/2/2022, DJe de 25/2/2022.

13. Julgados: REsp 2067181/PR, Rel. Ministra NANCY ANDRIGHI, TERCEIRA TURMA, julgado em 08/08/2023, DJe 15/08/2023; REsp n. 1.771.911/SP, relatora Ministra Nancy Andrichi, Terceira Turma, julgado em 16/3/2021, DJe de 26/4/2021.

14. LEONARDI, Marcel. *Responsabilidade civil dos provedores de serviços de internet*. Editora Juarez de Oliveira, 2005.

É possível também identificar em outros acórdãos do STJ o uso dos termos “sites de *e-commerce*”¹⁵ e “sites de intermediação”¹⁶. Ambos também fazem parte do grande grupo “aplicações da internet” do artigo 5º, inciso VIII do Marco Civil da Internet. No entanto, não parece que o legislador do art. 19, que estabelece o regime de responsabilidade subjetiva de provedores de aplicação por conteúdos de terceiros, realmente busque se referir a esses tipos de provedores, especialmente os sites de *e-commerce*, pois a natureza do serviço que prestam não tem publicações de terceiros como parte de seus modelos de negócio (ou, quando há, são apenas breves avaliações do produto adquirido).

Magistrados do Poder Judiciário constantemente deixam de fazer uso do termo “provedores de aplicação” em troca de termos que não estão previstos em normas, mas que denotam maior especificidade do serviço prestado na internet. Não é objetivo do presente artigo identificar diversos tipos de provedores de aplicação para que sejam regulados de formas distintas, no entanto eventual identificação de agrupamentos dentro desse termo, como já fazem alguns magistrados, não parece romper com as disposições do Marco Civil da Internet e contribuem para formulação de decisões que podem ser mais exatas.

2. O REGIME DE RESPONSABILIDADE CIVIL DE PROVEDORES DE APLICAÇÃO POR CONTEÚDOS DE TERCEIROS

Antes do Marco Civil da Internet, prevalecia o entendimento de que provedores de aplicação eram civilmente responsáveis por conteúdos de terceiros caso fossem notificados por um usuário e optassem pela manutenção do conteúdo¹⁷. Esse regime de responsabilidade civil, denominado *notice and down*, acarreta maior necessidade de avaliação de conteúdos por provedores de aplicação do que o regime imposto a partir do Marco Civil da Internet, no qual o provedor somente é responsável caso

15. REsp 2067181/PR, Rel. Ministra NANCY ANDRIGHI, TERCEIRA TURMA, julgado em 08/08/2023, DJe 15/08/2023.

16. REsp 1880344/SP, Rel. Ministra NANCY ANDRIGHI, TERCEIRA TURMA, julgado em 09/03/2021, DJe 11/03/2021.

17. PARENTONI, Leonardo Netto. Responsabilidade civil dos provedores de serviços na internet: Breves notas. *Âmbito Jurídico*, 2009.

descumpra uma ordem judicial para indisponibilização do conteúdo¹⁸. Esse regime é denominado *judicial notice and down*.

A escolha legislativa disposta no art. 19 do MCI privilegia o direito à liberdade de expressão e é uma barreira à responsabilidade civil de provedores de aplicação¹⁹. Anteriormente à legislação apontava-se a existência de um estímulo econômico à indisponibilização de conteúdos, já que a conduta protegeria o provedor de aplicação de eventual dever de reparação, fenômeno denominado de *chilling effect*²⁰, pois este “esfriaria” o debate nas redes.

Os artigos 21 e 31 do Marco Civil excepcionam a regra geral da responsabilidade civil de provedores de aplicação por conteúdos de terceiros. Em publicações que retratam nudez não consentida ou que contenham conteúdos que violem direitos autorais, prevalece a regra anterior ao MCI. Basta a notificação de um usuário e a manutenção do conteúdo para que o provedor possa ter de reparar o cidadão cujo direito foi violado. Nas hipóteses, o legislador optou por maior proteção ao bem jurídico tutelado.

É importante salientar que não foi imposta obrigação ao provedor de aplicação para que monitore conteúdos e os remova imediatamente após a publicação, ainda que possam fazer isso em conformidade com seus termos de uso, no qual informam a comunidade de usuários suas regras. Conforme Tarleton Gillespie aborda²¹, plataformas continuamente moderam conteúdos enquanto parte de seus modelos de negócios, de forma a tornar o ambiente virtual mais atrativo a seus usuários. As regras de responsabilidade civil dispostas no Marco Civil da Internet não impedem que provedores de aplicação moderem conteúdos, o que é feito em paralelo a pedidos de indisponibilização pela via judicial.

18. LEONARDI, Marcel. Internet e regulação: o bom exemplo do Marco Civil da Internet. *Revista do Advogado*, n. 115, 2012.

19. SOUZA, Carlos Affonso; TEFFÉ, Chiara Spadaccini de. Liberdade de Expressão e o Marco Civil da Internet. *TIC domicílios 2016: Pesquisa Sobre o Uso das Tecnologias de Informação e Comunicação nos Domicílios Brasileiros*.

20. KELLER, Daphne. Empirical Evidence of ‘Over-Removal’ by Internet Companies under Intermediary Liability Laws. *The Center for Internet and Society at Stanford Law School*, 2015.

21. GILLESPIE, Tarleton. *Custodians of the Internet: Platforms, content moderation, and the hidden decisions that shape social media*. Yale University Press, 2018.

A constitucionalidade do artigo 19 do Marco Civil da Internet é objeto de análise no Tema 987 do Supremo Tribunal Federal. Há grande debate se o artigo em análise não privilegia excessivamente a liberdade de expressão em detrimento de outros direitos fundamentais²², como a intimidade, honra e privacidade. Além disso, a profusão indiscriminada de desinformação em redes sociais mostrou-se um problema de ordem global, impactando diretamente processos eleitorais²³.

3. DECISÕES SINGULARES E A EVOLUÇÃO JURISPRUDENCIAL

Ao dissertar sobre a teoria jus-humanista normativa, o professor Thiago Lopes Matsushita exprime que a decisão mais justa resulta da interconexão entre o direito positivo, os direitos humanos e o realismo jurídico²⁴. O jus-humanismo normativo divide a norma em três dimensões - direito positivo, direito natural e realismo jurídico - que devem ser analisadas conjuntamente para as decisões judiciais. As três dimensões devem ser parte do processo decisório do operador do direito, de forma a viabilizar a construção e aplicação do ordenamento jurídico à realidade social²⁵.

A aplicação dos dispositivos do Marco Civil da Internet que regem a responsabilidade civil de provedores não é tarefa simples diante da realidade social. Modelos de negócios diversos, em consonância ao princípio da livre iniciativa reconhecida no artigo 3º, inciso VIII da lei emergem da internet²⁶, demonstrando seu caráter aberto, livre e de potencial disruptivo. Por vezes, litígios compostos por características imprevisíveis ao legislador do Marco Civil da Internet desafiam a aplicação da lei, ainda

22. HOBAlKA, Marcelo Bechara de Souza. A lei do atrito e a inconstitucionalidade do art. 19 do Marco Civil da Internet. *Jota*, 17 de mai. de 2024. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/a-lei-do-atrito-e-a-inconstitucionalidade-do-art-19-do-marco-civil-da-internet-17052024?non-beta=1>

23. EMPOLI, Giuliano da. 2020. *Os engenheiros do caos*. Tradução de Arnaldo Bloch. São Paulo: Vestígio.

24. MATSUSHITA, Thiago Lopes et al. O Jus-humanismo normativo expressão do princípio absoluto da proporcionalidade. 2012.

25. THEODORO JÚNIOR, Humberto. *Curso de Direito Processual Civil*—Volume I. rev. atual. Rio de Janeiro: Editora Forense, 2020.

26. RAHMAN, K. Sabeel; THELEN, Kathleen. The rise of the platform business model and the transformation of twenty-first-century capitalism. *Politics & society*, v. 47, n. 2, p. 177-204, 2019.

assim restando aos magistrados o dever de decidir.

É nesse contexto que serão analisadas no presente tópico decisões singulares que envolvem provedores de aplicação e conteúdos de terceiros. Foram escolhidos casos em que o objeto de análise dos magistrados não parecia se adequar ao que o legislador do Marco Civil da Internet previu ao reunir todos os provedores de aplicação em regra única sobre responsabilidade civil. Acredita-se que a decisão dá indícios de que a lei teve de ser conformada aos modelos de negócios desses provedores de aplicação e aos impactos que trazem à sociedade. Estudá-las é uma forma de conferir eventual necessidade de ajuste às normas de responsabilidade civil de intermediários, assim como reconhecer os acertos dos procedimentos previstos na lei. Além disso, busca-se observar se há um padrão nas decisões considerando que se tratam de provedores de aplicação cujos modelos de negócio são significativamente distintos entre si.

3.1. Provedores de pesquisa

O termo provedores de pesquisa, conforme já mencionado na introdução, é utilizado em decisões judiciais enquanto tipo de provedor de aplicação. Acredita-se que a escolha decorra das especificidades do serviço ofertado por aqueles que compõem este agrupamento, que agregam resultados de conteúdos de diversos sites, exercem controle sobre a forma de exibição dos resultados e sobre a ordem de cada um deles na relação disponibilizada aos usuários²⁷. O entendimento de que há um tipo de provedor entre o grande grupo provedores de aplicação foi objeto em tese do STJ:

“O provedor de pesquisa constitui uma espécie do gênero provedor de conteúdo, pois esses sites não incluem, hospedam, organizam ou, de qualquer outra forma, gerenciam as páginas virtuais indicadas nos resultados disponibilizados, apenas indicam links onde podem ser encontrados termos ou expressões de busca fornecidos pelo próprio usuário”²⁸.

27. DE OLIVEIRA COELHO, Júlia Costa. *Direito ao esquecimento e seus mecanismos de tutela na internet: como alcançar uma proteção real no universo virtual?*. Editora Foco, 2022.

28. Julgados: REsp 2012895/SP, Rel. Ministra NANCY ANDRIGHI, TERCEIRA TURMA, julgado em 08/08/2023, DJe 15/08/2023; REsp 1937989/SP, Rel. Ministro LUIS FELIPE SALOMÃO, QUARTA TURMA, julgado em 23/08/2022, DJe 07/11/2022; AgInt no AREsp 1085447/SP, Rel. Ministro RAUL ARAÚJO, QUARTA TURMA, julgado em 17/10/2022, DJe 21/10/2022 REsp

A tese também corrobora com o entendimento pacificado no STJ de que os resultados da pesquisa realizada nesse tipo de provedor de aplicação não são de sua responsabilidade e, portanto, eles não são parte legítima para figurar no polo passivo em pedido de indisponibilização do conteúdo. Os provedores de pesquisa “apenas indicam links”. Vejamos trecho de acórdão do TJ na Reclamação 5.072/AC²⁹ de 2014:

“(...) 3. Os provedores de pesquisa virtual realizam suas buscas dentro de um universo virtual, cujo acesso é público e irrestrito, ou seja, seu papel se restringe à identificação de páginas na web onde determinado dado ou informação, ainda que ilícito, estão sendo livremente veiculados. Dessa forma, ainda que seus mecanismos de busca facilitem o acesso e a consequente divulgação de páginas cujo conteúdo seja potencialmente ilegal, fato é que essas páginas são públicas e compõem a rede mundial de computadores e, por isso, aparecem no resultado dos sites de pesquisa.

4. Os provedores de pesquisa virtual não podem ser obrigados a eliminar do seu sistema os resultados derivados da busca de determinado termo ou expressão, tampouco os resultados que apontem para uma foto ou texto específico, independentemente da indicação do URL da página onde este estiver inserido”.

O entendimento em questão foi firmado no mesmo ano da promulgação do Marco Civil da Internet, no entanto foi citado em diversos julgamentos supervenientes, como o REsp 1771911/SP, o AgInt nos EDcl no AgInt no REsp 1754214/SP e no AgInt no AREsp 1227394/SP. É possível depreender que o entendimento adotado pela Corte foi de que o conteúdo filtrado e listado pelo provedor de pesquisa não é considerado um “conteúdo de terceiro”. As páginas indexadas pelo buscador não são compreendidas da mesma forma, por exemplo, que uma publicação em rede social, pois, se assim fossem, os provedores de pesquisa poderiam ser obrigados a indisponibilizar conteúdos que lista em suas páginas de resultados. Esse entendimento, inclusive, já era adotado anteriormente ao Marco Civil da Internet³⁰.

2006420/RJ (decisão monocrática), Rel. Ministra MARIA ISABEL GALLOTTI, QUARTA TURMA, julgado em 27/02/2023, publicado em 02/03/2023.

29. Rcl n. 5.072/AC, relator Ministro Marco Buzzi, relatora para acórdão Ministra Nancy Andrighi, Segunda Seção, julgado em 11/12/2013, DJe de 4/6/2014.

30. ANDRIGHI, Fátima Nancy. A responsabilidade civil dos provedores de pesquisa via internet. *Rev. TST*, Brasília, v. 78, n. 3, p. 64-75, 2012.

O modelo de negócio adotado por provedores de pesquisa faz com que os conteúdos que terceiros produzem e que são exibidos em seus resultados tenham características similares, mas não iguais, ao de outros provedores de aplicação. Evidentemente não deve ser exigido que o buscador exclua um conteúdo hospedado em outra página que não a sua, cujo titular é outro provedor de aplicação, no entanto, sendo provedores de pesquisa uma espécie dos provedores de aplicação, eles estão sujeitos às obrigações impostas a esse grande grupo, inclusive quanto ao artigo 19 do Marco Civil da Internet. Mesmo que não esteja normatizado com esse detalhamento, ao que parece, a aplicação do dispositivo se dá apenas em casos de conteúdos de terceiros que são produzidos e publicados dentro do próprio serviço do provedor de aplicação, diferenciando-se do modelo de negócio de provedores de pesquisa.

É passível de críticas a forma com que os magistrados interpretam a responsabilidade civil de provedores de pesquisa, pois parte-se de uma premissa que são meros agregadores de listagens de publicações de outros provedores de aplicação, sem que se leve em consideração a forma com que participam da construção do conhecimento público a partir de seus algoritmos que priorizam determinados resultados³¹. A tese firmada pelo STJ evidencia esse entendimento ao dispor que esses sites não organizam e nem gerenciam os resultados da busca. No entanto, em consulta à “Central de Ajuda” do buscador Google, têm-se a informação de que os resultados de pesquisas no provedor podem ser ajustados com base nas atividades anteriores do usuário, sua localização e idioma³², contrariando o entendimento adotado pelo STJ.

Dessa forma, para fins de responsabilidade civil, eventual conteúdo ilícito listado em buscadores pertence apenas ao provedor de aplicação que o hospeda. Ainda que o provedor de pesquisa agregue resultados e os torne muito mais acessíveis para usuários, eles não são responsáveis civilmente por conteúdos de terceiros. Cabe ao usuário que deseja a indisponibilização de um conteúdo que postule em face do provedor de aplicação que o divulgou primariamente, não ao provedor de pesquisa. O debate ilustra como é sensível legislar sobre tecnologias sujeitas a aprimoramentos

31. NOBLE, Safiya Umoja. Algorithms of oppression: How search engines reinforce racism. In: *Algorithms of oppression*. New York university press, 2018.

32. GOOGLE. Personalização e resultados da pesquisa do Google. Disponível em: <https://support.google.com/websearch/answer/12410098?hl=pt-pt>. Acesso em 17 jun. 2024.

contínuos e cujo modelo de negócio é inovador³³.

Outras teses correlatas a agregação de listagens de pesquisa também foi levada aos tribunais. O “direito ao esquecimento” foi o principal instituto jurídico evocado por cidadãos para que determinados resultados em buscadores fossem eliminados, sob o argumento de que se tratavam de fatos antigos que prejudicam a imagem de quem é associado ao resultado. Além do pedido de reparação pecuniária, os autores requereram a obrigação da eliminação do conteúdo desabonador da listagem de resultados da pesquisa. Não se requeria a indisponibilização do conteúdo na internet, apenas sua eliminação na base de dados do provedor de pesquisa.

No entanto, o Supremo Tribunal Federal (STF) entendeu em 2021, no Tema 786³⁴, que o direito ao esquecimento seria incompatível com a Constituição de 1988, pois se tratando de fatos verídicos, ainda que tenham ocorrido há longo tempo, devem seguir acessíveis. O caso de repercussão geral tratou da reconstituição de um crime que ocorreu em 1950 em um documentário de 2004. De acordo com os ministros, a liberdade de expressão consagrada e protegida no ordenamento jurídico brasileiro seria prejudicada em demasia com o acolhimento dessa tese.

Por fim, o direito ao esquecimento não deve ser confundido com o direito à desindexação. Foi o que entendeu o Superior Tribunal de Justiça no Recurso Especial 1.660.168/RJ³⁵ em 2022. Em decisão posterior ao Tema 786, os magistrados consideraram que seria cabível a desvinculação de conteúdos desabonadores exibidos enquanto resultado à pesquisa unicamente do nome de cidadãos. Conforme a decisão, o conteúdo impugnado deve seguir na base de dados do provedor de pesquisa e poderá ser exibido mediante pesquisa de outros termos, ainda que seja desvinculada a busca isolada ao nome do cidadão.

Os casos mencionados são interconectados pois são relacionados a disponibilização de conteúdos em provedores de aplicação. A regra geral do artigo 19 do Marco

33. SOUZA, Carlos Affonso; LEMOS, Ronaldo. *Marco civil da internet: construção e aplicação*. Juiz de Fora: Editar Editora Associada Ltda, 2016, p. 18.

34. STF - RE: 1010606 RJ, Relator: DIAS TOFFOLI, Data de Julgamento: 11/02/2021, Tribunal Pleno, Data de Publicação: 20/05/2021.

35. REsp n. 1.660.168/RJ, relator Ministro Marco Aurélio Bellizze, Terceira Turma, julgado em 21/6/2022, DJe de 30/6/2022.

Civil da Internet não se mostra adequada para aplicação ao modelo de negócio de buscadores, pois estes exibem conteúdos que não produzem e nem hospedam integralmente. A exclusão desses conteúdos da base de dados também se mostra inadequada, pois poderia impedir o acesso à informação. A solução jurídica encontrada, o “direito a desindexação”, ainda que esteja sujeita a reavaliação pelo STJ, se assemelha em partes ao regime estabelecido no Marco Civil da Internet: o provedor de pesquisa, motivado por decisão judicial, tornou indisponível a vinculação de um conteúdo desabonador a busca do nome de um cidadão.

Na jurisprudência que reconheceu o direito à desindexação, não há menção à reparação, ainda que acredite-se que seja possível o ajuizamento de ação com pedido de reparação caso a desvinculação não seja feita de modo integral e duradouro. Além disso, o conteúdo desabonador seguirá na internet, com circulação significativamente reduzida, já que os buscadores são fonte robusta e primária de pesquisa. Observa-se que uma interpretação literal do artigo 19 não se mostra aplicável aos provedores de pesquisa e que, em princípio, o direito reconhecido pelo STJ se mostra decisão mais acertada para equilibrar direitos em conflito em provedores de pesquisa.

3.2. Provedores de mensageria criptografados

Entre 2015 e 2016, foram proferidas quatro decisões judiciais determinando o bloqueio do provedor de aplicação WhatsApp, após a recusa em fornecer o conteúdo das conversas de seus usuários para investigações criminais. Das quatro decisões, apenas em duas os bloqueios chegaram a se concretizar, com duração de 4 e de 12 horas. Um dos casos em que a suspensão se deu antes da efetivação do bloqueio culminou na ADPF 403, de relatoria do ministro Edson Fachin, na qual a corte do Supremo Tribunal Federal decidirá se o bloqueio está de acordo com a ordem constitucional brasileira.

O descumprimento das ordens judiciais pelo WhatsApp é justificado por impossibilidade técnica de acesso às mensagens de seu usuário. Conforme a empresa informa em sua central de ajuda³⁶, as mensagens trocadas na plataforma são protegidas

36. WHATSAPP. *Perguntas frequentes sobre o WhatsApp*. [S.l.: s.n.], [s.d.]. Disponível em:

por um “cadeado” e apenas os participantes da conversa teriam acesso a essa “chave”. A criptografia inibe o acesso do WhatsApp não apenas ao teor das mensagens, mas de toda a conversa, de modo que não é possível identificar qual tipo de conteúdo foi enviado (texto, áudio, foto, vídeo, documentos), volume de conteúdos e nem muito menos o teor deles.

A criptografia de ponta a ponta é valorizada por organizações defensoras de direitos humanos por promover especial proteção à liberdade de expressão³⁷. Ainda que o provedor de aplicação não adote a criptografia, medidas de bloqueio geral são consideradas significativamente invasivas a direitos fundamentais de acesso e compartilhamento de informações³⁸, assim como desproporcionais ao afetar todos os usuários da aplicação. O bloqueio de aplicações também não parece ser medida tão eficaz por ser contornável com o uso de outros serviços ou de redes VPNs³⁹.

A ordem para que um provedor de aplicação disponibilize conteúdos de terceiros criptografados confronta limites técnicos. Conforme Lawrence Lessig aborda⁴⁰, a regulação do ecossistema digital pode ser mais eficaz se feita considerando também os códigos que fundamentam esses espaços e não apenas por leis. No caso em comento, ainda que o direito penal preveja institutos para obtenção de provas em investigações, o código do provedor de aplicação criptografado torna-se barreira intransponível, a não ser que seja trocado por outro. A tese do professor norte-americano é

https://faq.whatsapp.com/820124435853543/?locale=pt_BR. Acesso em: 03 jul. 2024.

37. DIREITOS NA REDE. *Em defesa da criptografia e da constitucionalidade do artigo 19 do Marco Civil da Internet no julgamento do STF sobre o WhatsApp*. 21 jun. 2023. Disponível em: <https://direitosnarede.org.br/2023/06/21/em-defesa-da-critpografia-e-da-constitucionalidade-do-artigo-19-do-marco-civil-da-internet-no-julgamento-do-stf-sobre-o-whatsapp/>. Acesso em: 03 jul. 2024.

38. ARTIGO 19. *Bloqueios de sites e aplicativos no Brasil – Subsídios ao debate legislativo*. São Paulo, 2017. Disponível em: <https://artigo19.org/wp-content/blogs.dir/24/files/2017/12/Bloqueios-de-sites-e-aplicativos-no-Brasil-%E2%80%93-Subs%C3%ADdios-ao-debate-legislativo.pdf>. Acesso em: 03 jul. 2024.

39. ANJOS, Lucas Costa dos. *Para além dos bloqueios do WhatsApp: suspender provedores de aplicação pode ser um caminho sem volta*. Instituto de Referência em Internet e Sociedade, 2017. Disponível em: <https://irisbh.com.br/para-alem-dos-bloqueios-do-whatsapp-suspender-provedores-de-aplicacao-pode-ser-um-caminho-sem-volta/>. Acesso em: 03 jul. 2024.

40. LESSIG, Lawrence. *CODE: Version 2.0*. New York: Basic Books, 2006.

que a execução da lei, por vezes, é delimitada por limites técnicos e que os códigos deveriam ser considerados no processo regulatório, o que é ilustrado com os casos em comento.

Retomando a discussão central da pesquisa, as mensagens trocadas por meio de aplicativos de mensageria devem ser consideradas “conteúdos de terceiros”? O provedor de mensageria deve ser responsável civilmente pelos conteúdos ilícitos que circulam de forma privada em sua plataforma? A quantidade de participantes de uma conversa, o que influencia seu grau de publicidade, deve ser considerada na definição do regime de responsabilidade do provedor que hospeda as informações?

Os bloqueios do WhatsApp foram respostas do poder judiciário ao inaccessos as mensagens ali trocadas. Uma vez que o provedor não acessa os conteúdos da conversa, ele não tem controle para gerenciar e indisponibilizar eventuais mensagens de terceiros consideradas ofensivas ou desinformativas. Os casos de bloqueio não se relacionam com responsabilidade civil do provedor de aplicação diretamente, no entanto servem como referência para a reflexão almejada. Como se percebe, a lógica do artigo 19 do Marco Civil da Internet não se mostra aplicável ao modelo de negócio desse provedor de aplicação, que é um dos mais utilizados no país.

Após as eleições de 2022, o Tribunal Superior Eleitoral exigiu que o WhatsApp excluísse grupos criados em para promoção de um golpe de Estado⁴¹. De acordo com a política de privacidade do provedor de aplicação, quando um grupo é criado na ferramenta é verificado se seu nome e descrição atendem aos requisitos da plataforma⁴². Acredita-se que foi protegido por essa política que o WhatsApp tenha identificado e excluído os grupos golpistas, mesmo sem acesso do provedor ao teor da conversa.

Por fim, o WhatsApp criou recentemente uma nova funcionalidade denominada

41. MELO, Patricia Campos. *TSE dá ordens em série para derrubar grupos golpistas que se multiplicam nas plataformas*. São Paulo, 12 nov. 2022. Poder. Disponível em: <https://www1.folha.uol.com.br/poder/2022/11/tse-da-ordens-em-serie-para-derrubar-grupos-golpistas-que-se-multiplicacao-nas-plataformas.shtml>. Acesso em: 03 jul. 2024.

42. WHATSAPP. *Why and how we process data*. [S.l.: s.n.], [202-?]. Disponível em: <https://www.whatsapp.com/legal/brazil-privacy-notice/why-and-how-we-process-data>. Acesso em: 03 jul. 2024.

“Canais”⁴³, que consistem em uma espécie de grupos públicos, que não são criptografados e que qualquer usuário pode localizar na plataforma, passar a seguir, visualizar e reagir ao conteúdo ali exposto. Em alguma medida, os canais se assemelham as redes sociais e podem ser uma nova etapa de amadurecimento jurisprudencial sobre decisões correlatas à responsabilidade civil de provedores de mensageria.

3.3. Proteção da criança e do adolescente

Em decisão de 2021, no Recurso Especial 1783269⁴⁴, o Superior Tribunal de Justiça (STJ) decidiu que o Facebook deveria reparar os autores da ação (pai e filho) retratados em uma foto publicada em sua rede acompanhada de mensagem que associava o genitor à prática de pedofilia. Antes da propositura da ação, os autores notificaram extrajudicialmente o provedor de aplicação, que respondeu que o conteúdo não violava seus termos de uso e que não o indisponibilizaria. O entendimento do Ministro Relator Antonio Carlos Ferreira foi seguido por mais quatro colegas, recebendo apenas um voto divergente. Entre outros pontos, a ementa do julgado dispôs que:

“(...) é dever do provedor de aplicação na rede mundial de computadores (Internet) proceder à retirada de conteúdo envolvendo menor de idade - relacionado à acusação de que seu genitor havia praticado crimes de natureza sexual - logo após ser formalmente comunicado da publicação ofensiva, independente de ordem judicial”.

A controvérsia do caso em questão repousa no aparente conflito entre a proteção à criança e genitor retratados, cuja foto perdurou na rede social em contexto negativo por longo período, e o regime de responsabilidade civil de provedores de aplicação previsto no Marco Civil da Internet. Se considerado apenas o artigo 19 da lei, não houve descumprimento à ordem judicial que exigisse a indisponibilização do conteúdo e, portanto, não seria cabível a aplicação desse mecanismo de responsabilidade

43. WHATSAPP. *Canais de WhatsApp*: política de privacidade. Disponível em: https://www.whatsapp.com/legal/channels-privacy-policy?lang=pt_BR#:~:text=Os%20Canais%20s%C3%A3o%20p%C3%BAblicos%2C%20o,qual-quer%20usu%C3%A1rio%20e%20pelo%20WhatsApp. Acesso em: 3 jul. 2024.

44. REsp 1783269/MG, Rel. Ministro ANTONIO CARLOS FERREIRA, QUARTA TURMA, julgado em 14/12/2021, DJe 18/02/2022.

civil.

A tese vencedora do julgamento aceitou o argumento de que seria insuficiente a aplicação isolada do art. 19 do Marco Civil da Internet e que ele deveria ser interpretado à luz do art. 5º, X, da Constituição Federal e das normas do Estatuto da Criança e do Adolescente. Diante da vulnerabilidade de crianças e adolescentes e do grau de proteção que o ordenamento jurídico confere a eles, seria o caso de aplicar o Marco Civil enquanto parte do arcabouço normativo brasileiro, dotado de outras regras e princípios orientativos.

O acórdão é fundamentado em outras normas, para além do Marco Civil da Internet, levando os magistrados a excepcionar a regra do regime de responsabilidade civil previsto na lei. A professora Ana Frazão afirmou que a decisão “propõe uma nova forma de se ver o problema, pois a simples conclusão de que o art. 19 do Marco Civil não pode ser interpretado de forma isolada já possibilita uma série de reflexões a partir do necessário diálogo com outras normas que, para além do ECA, também se aplicam às relações entre plataformas e usuários, como é o caso do CDC”⁴⁵. Ao decidirem com base em outras normas, os magistrados tornam tangíveis novas argumentações de que o Marco Civil da Internet não seria o único diploma normativo a ser aplicado para verificar a responsabilidade civil do provedor de aplicação e o dever de indisponibilizar determinados conteúdos.

Nesse mesmo sentido, argumentam os professores Fábio Queiroz Pereira e Mariana Alves Lara ao analisar a decisão⁴⁶, “não se trata de solução *contra legem*, mas de medida que enfoca o ordenamento jurídico de maneira integrada e sistemática, atendendo-se ao diálogo das fontes”. Ainda que a decisão possa ser considerada correta, é evidente que a linha argumentativa adotada inova quando comparada a outras decisões, pois confere responsabilidade civil ao provedor de aplicação por conteúdo de terceiros mesmo sem descumprimento da ordem judicial.

45. FRAZÃO, Ana. Algoritmos e inteligência artificial. *Jota*, 23 de fev. de 2022. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/responsabilidade-provedores-de-aplicacao-23022022>

46. PEREIRA, Fabio Queiroz; LARA, Mariana Alves. A responsabilidade civil dos provedores de aplicação por conteúdo envolvendo crianças e adolescentes: análise do REsp. n. 1.783. 269/MG. *Civillistica.com*, v. 11, n. 3, p. 1-11, 2022.

Seguindo a lógica argumentativa do acórdão em comento, é possível que provedores de aplicação sejam responsabilizados civilmente em caso de recebimento de notificação do usuário e não indisponibilização do conteúdo em outros contextos. A proteção e primazia da ordem democrática brasileira, assegurada na Constituição de 1988, também evoca um regime mais protetivo à regra geral do artigo 19 do Marco Civil da Internet? Publicações que discriminam minorias sociais também têm o condão de conferir responsabilidade civil aos provedores de conexão após a notificação do usuário?

A ementa do acórdão do caso em análise dispõe que é dever do provedor de aplicação notificado proceder a retirada de publicação ofensiva envolvendo menor de idade, sob pena de o indenizar. Ainda que a decisão não tenha isoladamente efeito vinculante, servirá de referência para todos os julgados com temática semelhante, o que evidencia sua relevância para todas as espécies de provedores de aplicação. O sistema processual brasileiro elevou a jurisprudência à categoria de fonte de direito, ainda que não possa funcionar como mecanismo de revogação ou de afastamento da lei⁴⁷.

O voto vencedor do ministro relator menciona características do modelo de negócio do provedor de aplicação que hospedou o conteúdo impugnado. O magistrado relata que a empresa foi notificada de uma publicação; que o autor da postagem denunciada adicionou todos os usuários que eram “amigos” do genitor na rede social; e que a publicação continha foto e texto. Tais características que compõem a argumentação do magistrado majoritariamente não são observadas em outros provedores de aplicação, constituídos de forma distinta.

A decisão, ainda que utilize a nomenclatura “provedores de aplicação”, busca remediar uma situação que em geral se repete apenas em redes sociais. Pontos centrais da decisão não são observados em outros prestadores de serviços na internet, como a possibilidade de se conectar a terceiros, publicar fotos com texto e, até mesmo, de notificar o provedor de aplicação. Além disso, redes sociais são caracterizadas pela veloz dispersão de conteúdo promovida por algoritmos, grande volume de usuários e possibilidade de engajamento de terceiros. Acredita-se que o modelo de negócio do provedor de aplicação do caso em análise possui características que ampliaram a

47. THEODORO JÚNIOR, Humberto. *Op. cit*, loc. cit.

necessidade de proteção à criança e adolescente.

4 CONSIDERAÇÕES FINAIS

A breve recuperação jurisprudencial realizada buscou evidenciar inquietações quanto à amplitude do termo “provedores de aplicação”, assim como retratar impactos da homogeneização de direitos e deveres impostos aos que compõem esse grupo. O aprofundamento do uso de tecnologias em sociedade traz cotidianamente novos contornos para as relações estabelecidas no ciberespaço, gerando também consequências jurídicas.

As decisões analisadas na terceira parte da pesquisa são parte de um grande grupo temático correlato à responsabilidade civil de provedores de aplicação por conteúdos de terceiros. Em geral, quando o poder judiciário é chamado a decidir sobre litígios correlatos a conteúdos de terceiros, tratam-se de publicações em redes sociais e o sistema estabelecido no MCI traz contornos claros para resolução de questões nesse campo. O provedor de aplicação somente será responsável civilmente se descumprir uma ordem judicial de indisponibilização do conteúdo.

No entanto, as particularidades dos diversos modelos de negócios presentes entre provedores de aplicação fazem com que magistrados, por vezes, tenham de decidir em cenário de elevada complexidade jurídica. São diversos pontos em debate efervescente, como nos casos em que produtos são qualificados enquanto conteúdos de terceiros. Essa foi a interpretação do Superior Tribunal de Justiça no Recurso Especial nº 1.444.008/RS, que afastou a responsabilidade civil de um provedor de aplicações que catalogava produtos para facilitar a compra por consumidores⁴⁸.

Outros casos ainda pendem de decisão, como a responsabilidade civil de provedores de aplicação que agregam e facilitam acesso à conteúdos de processos judiciais⁴⁹. Amparados pelo princípio da publicidade processual, esses provedores salvam

48. FALEIROS JÚNIOR, José Luiz de Moura; LONGHI, João Victor Rozatti. A responsabilidade civil dos provedores de busca de produtos na internet. *Revista da Faculdade de Direito da UERJ-RFD*, n. 37, p. 75-95, 2020.

49. VILELA, Gustavo Baião. A responsabilidade civil pela divulgação na internet de informações processuais (Tema 1141 do STF). In PARENTONI, Leonardo (Coord). “*Direito, Tecnologia e Inovação – v. IV: Estudos de caso*”. Belo Horizonte: Editora Expert, 2022.

e exibem em suas ferramentas processos de terceiros, o que pode lhes acarretar obstáculos pessoais e profissionais. O Tema 1141 do STF aguarda ser pautado para que os ministros decidam sobre a responsabilidade civil de provedores de aplicação por disponibilização de informações processuais publicadas nos órgãos oficiais do Poder Judiciário.

A pesquisa proposta buscou responder se é possível que todos os provedores de aplicação recebam igual tratamento jurídico quanto ao regime de responsabilidade civil por conteúdos de terceiros. Como se percebe dos casos colacionados, particularidades dos modelos de negócios podem tornar isso tecnicamente inviável, como é o caso do provedor de mensageria que adota a criptografia. Ainda, a interpretação sistêmica do arcabouço jurídico brasileiro pode justificar a insuficiência de aplicar apenas a norma do artigo 19.

Por fim, ainda que o Marco Civil da Internet seja dispositivo de grande importância na busca da homogeneização das decisões em litígios *online*, é natural que alguns pontos sejam aperfeiçoados após dez anos de sua promulgação. O regime de responsabilidade civil previsto no artigo 19 é de grande valor para preservação do modelo de negócio de provedores de rede social, no entanto não parece ser suficiente para abranger todos os provedores de aplicações.

REFERÊNCIAS

- ANDRIGHI, Fátima Nancy. A responsabilidade civil dos provedores de pesquisa via internet. *Rev. TST*, Brasília, v. 78, n. 3, p. 64-75, 2012.
- ANJOS, Lucas Costa dos. *Para além dos bloqueios do WhatsApp: suspender provedores de aplicação pode ser um caminho sem volta*. Instituto de Referência em Internet e Sociedade, 2017. Disponível em: <https://irisbh.com.br/para-alem-dos-bloqueios-do-whatsapp-suspender-provedores-de-aplicacao-pode-ser-um-caminho-sem-volta/>. Acesso em: 03 jul. 2024.
- ARTIGO 19. *Bloqueios de sites e aplicativos no Brasil – Subsídios ao debate legislativo*. São Paulo, 2017. Disponível em: <https://artigo19.org/wp-content/blogs.dir/24/files/2017/12/Bloqueios-de-sites-e-aplicativos-no-Brasil-%E2%80%93-Subs%C3%ADdios-ao-debate-legislativo.pdf>. Acesso em: 03 jul. 2024.
- BENTES, Ana. *A gestão algorítmica da atenção: Enganchar, Conhecer e Persuadir*. In: Seminário Governança das Redes, 4., 2019, Belo Horizonte. Políticas, Internet e Sociedade. Belo Horizonte: IRIS. p. 222-234.

- BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece Princípios, garantias, direitos e deveres para o uso da internet no Brasil. *Diário Oficial da União*: Brasília, DF, 23 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 10 de mai. 2024.
- CASTELLS, Manuel. *A Galáxia Internet: reflexões sobre a Internet, negócios e a sociedade*. Zahar, 2003.
- CEROY, Frederico Meinberg. Os conceitos de provedores no Marco Civil da Internet. *Revista Eletrônica Direito & TI*, v. 1, n. 1, p. 3-3, 2015.
- DE OLIVEIRA COELHO, Júlia Costa. *Direito ao esquecimento e seus mecanismos de tutela na internet: como alcançar uma proteção real no universo virtual?*. Editora Foco, 2022.
- DIREITOS NA REDE. *Em defesa da criptografia e da constitucionalidade do artigo 19 do Marco Civil da Internet no julgamento do STF sobre o WhatsApp*. 21 jun. 2023. Disponível em: <https://direitosnarede.org.br/2023/06/21/em-defesa-da-critpografia-e-da-constitucionalidade-do-artigo-19-do-marco-civil-da-internet-no-julgamento-do-stf-sobre-o-whatsapp/>. Acesso em: 03 jul. 2024.
- EMPOLI, Giuliano da. *Os engenheiros do caos*. Tradução de Arnaldo Bloch. São Paulo: Vestígio, 2020.
- FALEIROS JÚNIOR, José Luiz de Moura; LONGHI, João Victor Rozatti. A responsabilidade civil dos provedores de busca de produtos na internet. *Revista da Faculdade de Direito da UERJ-RFD*, n. 37, p. 75-95, 2020.
- FERNANDES, André (s.d.). Disponível em: <https://ip.rec.br/blog/provedores-de-conteudo-e-aplicacao-interpretacao-do-marco-civil-da-internet/>. Acesso em: 10 de mai. 2024.
- FRAZÃO, Ana. Algoritmos e inteligência artificial. *Jota*, 23 de fev. de 2022. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/responsabilidade-provedores-de-aplicacao-23022022>
- GILLESPIE, Tarleton. *Custodians of the Internet: Platforms, content moderation, and the hidden decisions that shape social media*. Yale University Press, 2018.
- GOOGLE. *Personalização e resultados da pesquisa do Google*. Disponível em: <https://support.google.com/websearch/answer/12410098?hl=pt-pt>. Acesso em 17 jun. 2024.
- HOBAlKA, Marcelo Bechara de Souza. A lei do atrito e a inconstitucionalidade do art. 19 do Marco Civil da Internet. *Jota*, 17 mai. de 2024. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/a-lei-do-atrito-e-a-inconstitucionalidade-do-art-19-do-marco-civil-da-internet-17052024?non-beta=1>.
- KELLER, Daphne. Empirical Evidence of ‘Over-Removal’ by Internet Companies under Intermediary Liability Laws. *The Center for Internet and Society at Stanford Law School*, 2015.
- LEONARDI, Marcel. Internet e regulação: o bom exemplo do Marco Civil da Internet. *Revista do Advogado*, n. 115, 2012.
- LESSIG, Lawrence. *CODE: Version 2.0*. New York: Basic Books, 2006.

- MATSUSHITA, Thiago Lopes *et al.* *O Jus-humanismo normativo expressão do princípio absoluto da proporcionalidade*. 2012.
- NOBLE, Safiya Umoja. Algorithms of oppression: How search engines reinforce racism. In: *Algorithms of oppression*. New York university press, 2018.
- NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR. (2023). *Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros: pesquisa TIC Domicílios*, ano 2022. Disponível em: <https://cetic.br/pt/arquivos/domicilios/2022/domicilios/>.
- PARENTONI, Leonardo Netto. Responsabilidade civil dos provedores de serviços na internet: Breves notas. *Âmbito Jurídico*, 2009.
- PEREIRA, Fabio Queiroz; LARA, Mariana Alves. A responsabilidade civil dos provedores de aplicação por conteúdo envolvendo crianças e adolescentes: análise do REsp. n. 1.783. 269/MG. *Civilistica.com*, v. 11, n. 3, p. 1-11, 2022.
- RAHMAN, K. Sabeel; THELEN, Kathleen. The rise of the platform business model and the transformation of twenty-first-century capitalism. *Politics & society*, v. 47, n. 2, p. 177-204, 2019.
- SOUZA, Carlos Affonso; LEMOS, Ronaldo. *Marco Civil da Internet: construção e aplicação*. Juiz de Fora: Editar Editora Associada Ltda, 2016, p. 18.
- SOUZA, Carlos Affonso; TEFFÊ, Chiara Spadaccini de. Liberdade de Expressão e o Marco Civil da Internet. *TIC domicílios 2016: Pesquisa Sobre o Uso das Tecnologias de Informação e Comunicação nos Domicílios Brasileiros*.
- THEODORO JÚNIOR, Humberto. *Curso de Direito Processual Civil*—Volume I. rev. atual. Rio de Janeiro: Editora Forense, 2020.
- VILELA, Gustavo Baião. A responsabilidade civil pela divulgação na internet de informações processuais (Tema 1141 do STF). In PARENTONI, Leonardo (Coord). “*Direito, Tecnologia e Inovação* – v. IV: Estudos de caso”. Belo Horizonte: Editora Expert, 2022.
- WHATSAPP. *Canais de WhatsApp: política de privacidade*. Disponível em: https://www.whatsapp.com/legal/channels-privacy-policy?lang=pt_BR#:~:text=Os%20Canais%20s%C3%A3o%20p%C3%BAblicos%2C%20o,qual-quer%20usu%C3%A1rio%20e%20pelo%20WhatsApp. Acesso em: 3 jul. 2024.
- WHATSAPP. *Perguntas frequentes sobre o WhatsApp*. [S.l.: s.n.], [s.d.]. Disponível em: https://faq.whatsapp.com/820124435853543/?locale=pt_BR. Acesso em: 03 jul. 2024.
- WHATSAPP. *Why and how we process data*. [S.l.: s.n.], [s.d.]. Disponível em: <https://www.whatsapp.com/legal/brazil-privacy-notice/why-and-how-we-process-data>. Acesso em: 03 jul. 2024.

V

MODERAÇÃO DE CONTEÚDO, LIBERDADE DE EXPRESSÃO E DIREITOS FUNDAMENTAIS

SHADOWBANNING: UMA TÉCNICA CONTROVERSA DE MODERAÇÃO DE CONTEÚDO DIGITAL

Fernanda Sathler Rocha Franco

Doutoranda em Direito na linha interdisciplinar de Tecnologia e Inovação na
Universidade Federal de Minas Gerais, mestra em Direito com ênfase em Inovação e
bacharelada em Ciências Humanas pela Universidade Federal de Juiz de Fora,
advogada.

DOI: <https://doi.org/10.59224/dti7.ch8>

Resumo: A moderação de conteúdos nas plataformas digitais tornou-se uma questão de primeira ordem nestes ambientes virtuais, considerando a crescente relevância e os diferentes impactos que tais conteúdos podem gerar. Neste cenário os provedores de conteúdo desempenham um papel cada vez maior, por meio de seus termos e políticas de uso, quanto à disciplina das regras e dos requisitos da moderação, além das diferentes formas de se moderar, a exemplo do *shadowbanning*, prática esta controversa, cujos critérios e operação costumam ser desconhecidos pelo usuário e pelo público geral. Diante disso, por meio dos métodos bibliográfico e documental, este artigo buscou analisar e compreender como a prática do *shadowbanning* é abordada sob a perspectiva jurídico-regulatória e quais são os aspectos normativos assegurados em relação a este tema, com ênfase na análise das seguintes normativas: *Digital Services Act* (DSA) e *Marco Civil da Internet* (MCI). Conclui-se que, embora contemple expressamente o tema do *shadowbanning* e preveja determinadas regras sobre o assunto, por outro lado, o DSA não disciplinou as diretrizes sobre a operação, a procedimentalização desta prática de moderação. Já o MCI, em que pese prever um conjunto principiológico e normativo de garantias do usuário da internet e das plataformas

Abstract: Content moderation on digital platforms has become a major issue in these virtual environments, considering the growing relevance and the different impacts that such content can generate. In this scenario, content providers play an increasing role, through their terms and policies of use, regarding the discipline of the rules and requirements of moderation, in addition to the different ways of moderating, such as *shadowbanning*, a controversial practice, whose criteria and operation are usually unknown to the user and the general public. Therefore, through bibliographic and documentary methods, this article sought to analyze and understand how the practice of *shadowbanning* is approached from a legal-regulatory perspective and what are the normative aspects ensured in relation to this theme, with emphasis on the analysis of the following regulations: *Digital Services Act* (DSA) and *Civil Rights Framework for the Internet* (MCI). It is concluded that, although it expressly contemplates the issue of *shadowbanning* and provides certain rules on the subject, on the other hand, DSA did not discipline the guidelines on the operation, the proceduralization of this practice of moderation. On the other hand, MCI, despite providing a principled and normative set of guarantees for the user of the internet and digital platforms, still adopts

digitais, ainda adota uma lógica binária em termos de moderação (remover ou não remover o conteúdo), desconsiderando outras formas intermediárias de moderar, incluindo o próprio *shadowbanning*. Sendo assim, conclui-se ainda que a tendência, nas plataformas digitais, seria o fortalecimento dos contratos (termos de uso) como ferramenta de sistematização e disciplina das diretrizes da moderação de conteúdo, como o *shadowbanning* e a consequente necessidade de adoção de uma perspectiva mais sistêmica, incluindo um maior diálogo das fontes e normas jurídicas civis, consumeristas, relacionadas aos direitos do usuário da internet e à proteção de dados pessoais no ambiente digital para fornecer um tratamento jurídico mais robusto ao tema da moderação de conteúdo e às suas variações, como o *shadowbanning*.

Palavras-chave: plataformas digitais, moderação de conteúdo, *shadowbanning*.

a binary logic in terms of moderation (removing or not removing content), disregarding other intermediate forms of moderation, including shadowbanning itself. Thus, it is also concluded that the tendency, in digital platforms, would be the strengthening of contracts (terms of use) as a tool for systematization and discipline of content moderation guidelines, such as shadowbanning and the consequent need to adopt a more systemic perspective, including a greater dialogue between sources and civil, consumerist legal norms related to the rights of internet users and the protection of personal data in the digital environment to provide a more robust legal treatment to the topic of content moderation and its variations, such as shadowbanning.

Keywords: digital platforms, content moderation, *shadowbanning*.

SUMÁRIO: 1. Introdução; 2. *Shadowbanning* nas plataformas digitais: forma de moderação de conteúdo, “curadoria” de conteúdo ou espécie de sanção imposta ao usuário?; 2.1 Algumas delimitações conceituais desta prática; 2.2 *Shadowbanning*: procedimento e principais aplicações; 3. Aspectos regulatórios do *shadowbanning*: observação normativa a partir do *Digital Services Act* (DSA) e do Marco Civil da Internet; 3.1 *Digital Services Act* (DSA); 3.2 Marco Civil da Internet (MCI); 4. Código Civil, Código de Defesa do Consumidor e Lei Geral de Proteção de Dados como possíveis fundamentos jurídicos para a abordagem do *shadowbanning*: prós e contras; 4.1 Código Civil e a teoria do abuso de direito; 4.1.1 *Shadowbanning* nas plataformas digitais: O caso Marcela Balandez x Facebook; 4.2 Código de Defesa do Consumidor (CDC): direito de transparência do usuário-consumidor quanto à prática de *shadowbanning*; 4.3 Lei n. 13.709/18 (Lei Geral de Proteção de Dados): direito à transparência e direito à revisão de decisões automatizadas sobre a prática de *shadowbanning*; 4.4 Projeto de Lei n. 2630/2020 - Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet; 5. Discussão e conclusão; Referências.

1. INTRODUÇÃO

Lidar com os potenciais e os riscos ofertados por conteúdos online tornou-se um dos principais desafios em termos jurídico-regulatórios, de governança da informação e do conteúdo. Some-se a isso o complexo papel que as grandes plataformas digitais¹, como redes sociais e outros canais de comunicação, aliadas a sofisticadas tecnologias de automação, vem progressivamente assumindo em relação à moderação² dos conteúdos veiculados pelos usuários destas plataformas.³

Por sua vez, a moderação automatizada de conteúdo tem sido implementada de diferentes formas, a exemplo do *shadowbanning*⁴ (*banimento à sombra* ou *banimento*

1. O termo *grandes plataformas digitais*, utilizado neste trabalho, equivale à expressão *very large on-line platforms* (VLOPs), que está prevista na recente diretiva europeia *Digital Services Act* (DSA) e se refere a plataformas de grande escala como YouTube, Meta, Instagram, TikTok, X (Twitter) e Facebook (QUINTAIS, João P.; APPELMAN, Naomi; FATHAIGH, Ronan Ó. Using Terms and Conditions to apply Fundamental Rights to Content Moderation. *German Law Journal*, 24, pp. 881–911, 2023. p. 883. Disponível em: <https://www.cambridge.org/core/journals/german-law-journal/article/using-terms-and-conditions-to-apply-fundamental-rights-to-content-moderation/B30B9043D1C6F14AE9C3647A845E6E10>. Acesso em 17 jun. 2024).
2. De acordo com o art. 3(t) do Digital Services Act (DSA), a moderação de conteúdo pode ser compreendida como um conjunto de “atividades, automatizadas ou não, empreendidas por prestadores de serviços intermediários, destinadas em especial a detectar, identificar e combater os conteúdos ilegais ou informações incompatíveis com os seus termos e condições fornecidos pelos destinatários do serviço, incluindo as medidas tomadas que afetam a disponibilidade, visibilidade e acessibilidade desses conteúdos ilegais ou dessas informações, como a despromoção, a desmone-tização, a desativação do acesso ou a supressão dos mesmos, ou que afetem a capacidade de os destinatários do serviço fornecerem essas informações, como a cessação ou suspensão da conta de um destinatário” (EUROPEAN UNION. Digital Services Act. *REGULATION (EU) 2022/2065 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC* (Digital Services Act). Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065>. Acesso em 13 jun. 2024).
3. MULLIGAN, Deirde, K.; BAMBERGER, Kenneth A. Allocating Responsibility in Content Moderation: A Functional Framework. *Berkeley Technology Law Journal*. Berkeley: University of California School of Law. v. 36, n. 03, p. 1091-1171, 2021. p. 1094.
4. Exemplificativamente, na plataforma “X” (Twitter), é possível identificar alguns exemplos de contas que foram afetadas pelo shadowbanning: a) Jay Bhattacharya, professor da Universidade de Stanford, ao afirmar, durante a pandemia da Covid-19, que o *lockdown* poderia prejudicar as

fantasma, em traduções literais), prática esta que limita a visibilidade, reduz o alcance do conteúdo veiculado pelo usuário de uma plataforma, sem que este usuário saiba disso prévia ou imediatamente⁵. Além disso, pouco ou praticamente nada se conhece sobre os critérios e o procedimento adotados pelas plataformas digitais na moderação de conteúdo e na prática de *shadowbanning*⁶.

Por outro lado, há quem defenda que o *shadowbanning* seria apenas uma espécie de “curadoria” dos conteúdos e não uma medida de rebaixamento imposta ao usuário em razão de suposto conteúdo violador das diretrizes e termos de uso das plataformas ou em razão de conteúdo que não tenha alcançado o engajamento desejado nas plataformas digitais.

Trata-se de uma prática sutil com implicações importantes, que incluem potenciais tratamentos discriminatórios ilícitos entre usuários, indisponibilização do acesso a informações relevantes, enviesamento de conteúdos, entre outras questões.⁷

crianças, teve sua conta movida para a “Trends Blacklist”, uma lista que impede os tweets de se tornarem tendência na rede; b) O influenciador de direita Dan Bongino teve sua conta incluída na “Search Blacklist”, o que prejudicou os resultados de busca por seu perfil; c) Por sua vez, a conta do ativista conservador Charlie Kirk recebeu o rótulo “Não amplificar” (SPAGNUOLO, Sergio. Twitter confirma shadow ban contra certos usuários. Núcleo, dez. 2022. Disponível em: <https://nucleo.jor.br/reportagem/2022-12-09-twitter-files-black-lists/>. Acesso em 17 jun. 2024).; Já o TikTok teria orientado seus funcionários a marcar os vídeos de pessoas com deficiências físicas, desfiguração facial, autismo e síndrome de Down, além de pessoas obesas, e segmentar estes usuários como “especiais” (FERNANDES, Rodrigo. Seis polêmicas do TikTok em 2019. Techtudo, dez. 2019. Disponível em: <https://www.techtudo.com.br/noticias/2019/12/seis-polemicas-do-tiktok-em-2019.ghtml>. Acesso em 17 jun. 2024).

5. CHEN, Yen-Shao; ZAMAN, Tauhid. Shaping opinions in social networks with shadow banning. *Plos One*, 19, 3, 2024. p. 2. Disponível em: <https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0299977>. Acesso em 15 jun. 2024.; ENARSSON, Therese. Online Content Moderation in and Beyond the EU Digital Services Act – Exploring the Tension between Automated Speed and Human Contextuality. SSRN, abr. 2024. p. 6. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4806704. Acesso em 15 jun. 2024.
6. LEE, Edward. Moderating Content Moderation: A Framework for Nonpartisanship in Online Governance. *American University Law Review*. Washington: Washington College of Law. v. 70, n. 03, p. 913-1060, fv. 2021. p. 913.
7. CHEN, Yen-Shao; ZAMAN, Tauhid. Shaping opinions in social networks with shadow banning. *Plos One*, 19, 3, 2024. p. 22. Disponível em:

Diante disso, este artigo buscou analisar e compreender como a prática do *shadowbanning* é abordada sob a perspectiva jurídico-regulatória e quais são os aspectos normativos assegurados em relação a este tema, com ênfase na análise das seguintes normativas: *Digital Services Act* (DSA) e Marco Civil da Internet (MCI).⁸

Como metodologia, adotou-se a pesquisa bibliográfica e documental, por meio da análise do Regulamento n. 2065/2022 (*Digital Services Act* - DSA), do Parlamento Europeu, e da Lei n. 12.965/2014 (Marco Civil da Internet - MCI) e discussão dos resultados com base em referencial teórico.

O trabalho está organizado da seguinte forma: após a introdução, aborda-se o conceito e o procedimento do *shadowbanning* nas plataformas digitais. Em seguida, é explorado o tratamento normativo conferido à esta prática, com ênfase no *Digital Services Act* (DSA) e no Marco Civil da Internet (MCI), além dos desafios tecnológicos impostos às iniciativas regulatórias sobre o tema, com apresentação das principais tecnologias subjacentes à moderação de conteúdo digital, incluindo o *shadowbanning*, com posterior apresentação de algumas das medidas disponibilizadas pelo Código Civil, Código de Defesa do Consumidor e Lei Geral de Proteção de Dados que podem contribuir para o tratamento jurídico do *shadowbanning* no Brasil, além da apresentação de alguns elementos relevantes para a moderação de conteúdo a partir do Projeto de Lei n. 2630/202. Por fim, discute-se algumas observações feitas a partir do estudo, com posterior conclusão.

2. SHADOWBANNING NAS PLATAFORMAS DIGITAIS: FORMA DE MODERAÇÃO DE CONTEÚDO, "CURADORIA" DE CONTEÚDO OU ESPÉCIE DE SANÇÃO IMPOSTA AO USUÁRIO?

<https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0299977>. Acesso em 15 jun. 2024.

8. No presente trabalho optou-se por essas normativas tendo em vista que o DSA é uma diretiva internacional que trata da moderação de conteúdo digital, além de ter sido a pioneira na abordagem expressa do *shadowbanning*. Por sua vez, optou-se pelo MCI por ser este o principal dispositivo de lei brasileiro que contempla os princípios e direitos dos usuários na internet e no meio virtual.

2.1 Algumas delimitações conceituais desta prática

Em linhas gerais, *shadowbanning* é um termo coloquial para descrever a situação em que determinada publicação de um usuário, em uma plataforma digital, deixa de ser visível aos demais usuários. Trata-se de uma estratégia utilizada pelas plataformas para reduzir a visibilidade do conteúdo nos mecanismos de busca e recomendação.⁹

Desta forma, o *shadow banning* tem sido aplicado de forma suplementar às estratégias comuns de moderação, como uma ferramenta de administração de controvérsias que envolvam violação das diretrizes das plataformas, em especial, em casos de conteúdos suspeitos de disseminar desinformação e discursos de ódio.

Todavia, se trata de uma prática que vem despertando a atenção não só dos usuários, mas também de estudiosos, por algumas razões, entre as quais o fato de que, em um primeiro momento, não se consegue saber se o seu próprio conteúdo foi alvo de *shadowbanning*¹⁰, em razão da ausência de notificação por parte das plataformas e do desconhecimento do público geral sobre o funcionamento desta prática¹¹. Logo, o usuário pode ter apenas a falsa impressão de que sua publicação continua visível na plataforma.

Regra geral, os termos e políticas de uso destas plataformas são os principais instrumentos que disciplinam sobre a utilização da plataforma e as interações dos

9. COTTER, Kelley. “Shadowbanning is not a thing”: black box gaslighting and the power to independently know and credibly critique algorithms. *Information, Communication & Society*, v. 26, 2023. Disponível em: <https://www.tandfonline.com/doi/full/10.1080/1369118X.2021.1994624>. Acesso em 12 jun. 2024.

10. Conforme elucidado por Gabriel Nicholas: “(...) exogenously determining whether an individual is really shadowbanned (not to mention evaluating more macro trends) is nearly impossible, since from the end users’ perspective, shadowbanning often looks identical to a technical glitch or a post being simply unpopular.” (NICHOLAS, Gabriel. *Sunsetting “Shadowbanning”*. *Yale Law School Information Society Project Platform Governance Terminologies Essay Series*, jul. 2023. p. 4. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4522168. Acesso em 17 jun. 2024).

11. NICHOLAS, Gabriel. *Sunsetting “Shadowbanning”*. *Yale Law School Information Society Project Platform Governance Terminologies Essay Series*, jul. 2023. p. 4. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4522168. Acesso em 17 jun. 2024.

usuários. Por outro lado, mesmo essas diretrizes¹², combinadas a práticas algorítmicas, costumam não esclarecer sobre o procedimento da moderação de conteúdo e, muito menos, do *shadowbanning*¹³, conforme apontado por Edward Lee, estudioso dos direitos da internet¹⁴.

Desta forma, torna-se desafiador definir o que realmente seria o *shadowbanning*: o resultado de um procedimento de moderação e classificação de conteúdo? Uma sanção imposta ao usuário? Uma espécie de curadoria de conteúdo? Um conjunto destes elementos?¹⁵

Para alguns autores, como Kelley Cotter, *shadowbanning* não é uma forma de moderação de conteúdo, pois sua aplicação não é informada aos usuários. Para a autora, esta prática seria uma modalidade mais suave de sanção imposta pelas

-
12. Sobre o tema, a título exemplificativo, vale destacar a diretriz “Para você”, recurso utilizado pelo TikTok em seu sistema de personalização da experiência do usuário. Resumidamente, seus termos são os seguintes: “Determinados tipos de conteúdo podem ser bons se vistos ocasionalmente, mas problemáticos se visualizados em sequência. Isso inclui conteúdo como dietas, condicionamento físico extremo, conteúdo sexualmente sugestivo, tristeza (como declarações de desesperança ou compartilhamento de citações tristes) e informações de saúde mental excessivamente generalizadas (como um questionário que alega diagnosticar alguém). Esse tipo de conteúdo poderá ser elegível para o feed “Para você”, mas interromperemos os padrões de conteúdo repetitivo para garantir que não seja visto com muita frequência. Saiba mais sobre nossa abordagem para proteger e diversificar recomendações.”. Esta diretriz do TikTok é um bom exemplo da ingerência que as plataformas digitais possuem tanto sobre os conteúdos entregues aos usuários quanto sobre a frequência de disponibilização dos mesmos, a partir de critérios majoritariamente definidos pelas próprias plataformas.
 13. QUINTAIS, João P.; APPELMAN, Naomi; FATHAIGH, Ronan Ó. Using Terms and Conditions to apply Fundamental Rights to Content Moderation. *German Law Journal*, 24, p. 881–911, 2023. p. 884. Disponível em: <https://www.cambridge.org/core/journals/german-law-journal/article/using-terms-and-conditions-to-apply-fundamental-rights-to-content-moderation/B30B9043D1C6F14AE9C3647A845E6E10>. Acesso em 17 jun. 2024.
 14. LEE, Edward. Moderating Content Moderation: A Framework for Nonpartisanship in Online Governance. *American University Law Review*. Washington: Washington College of Law. v. 70, n. 03, p. 913-1060, fv. 2021. p. 913.
 15. THORSON, Kjerstin; WELLS, Chris. Curated Flows: A Framework for Mapping Media Exposure in the Digital Age. *Communication Theory*, v. 26, i. 3, ago. 2016. Disponível em: <https://doi.org/10.1111/comt.12087>. Acesso em 13 jun. 2024.

plataformas digitais¹⁶.

Em compreensão diversa, Joan Donovan, Danah Boyd¹⁷, David Bamman, Brendan O'Connor e Noah Smith¹⁸ entendem que *shadowbanning* é uma das modalidades de censura algorítmica estratégica e silenciosa para evitar ações mais chamativas, como a suspensão das contas dos usuários.

Outra possibilidade de compreensão desta expressão é defendida por autores como Paddy Leerssen, para quem *shadowbanning* seria uma nova técnica de moderação de conteúdo nas plataformas digitais, por meio de sistemas de ranking dinâmicos e voláteis cujos efeitos ainda não são completamente conhecidos¹⁹. O presente trabalho adotará esta delimitação conceitual.

A seguir serão abordados alguns aspectos sobre a prática e as principais aplicações de *shadowbanning*.

2.2 *Shadowbanning*: procedimento e principais aplicações

O procedimento de *shadowbanning* é administrado por complexos sistemas de recomendação e busca, cujas interações são modeladas por algoritmos de otimização

-
16. COTTER, Kelley. Playing the Visibility Game: How Digital Influencers and Algorithms Negotiate Influence on Instagram. *New Media and Society*, 21, 4, p. 895-913, 2019. p. 16. Disponível em: <https://www.semanticscholar.org/paper/Playing-the-visibility-game%3A-How-digital-and-on-Cotter/3f94845cfec2ed04bfd0d0b1a41b994a56e5f6d9>. Acesso em 29 jun. 2024.
 17. DONOVAN, Joan; BOYD, Danah. Stop the Presses? Moving from Strategic Silence to Strategic Amplification in a Networked Media Ecosystem. *American Behavioral Scientist*, 65, 2, p. 333-350, 2019. Disponível em: https://www.researchgate.net/publication/356909505_Stop_the_Presses_Moving_from_Strategic_Silence_to_Strategic_Amplification_in_a_Networked_Media_Ecosystem. Acesso em 29 jun. 2024.
 18. BAMMAN, David; O'CONNOR, Brendan; SMITH, Noah A. Censorship and Deletion Practices in Chinese Social Media. *First Monday*, 17, 3, mar. 2012. p. 1-2. Disponível em: <https://www.semanticscholar.org/paper/Censorship-and-deletion-practices-in-Chinese-social-Bamman-O%27Connor/7c23d25d45b6bf781df6e1975674489604e388e4>. Acesso em 29 jun. 2024.
 19. LEERSSEN, Paddy. An end to shadow banning? Transparency rights in the Digital Services Act between content moderation and curation. *Computer Law & Security Review*, 48, p. 1-13, 2023. p. 11. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0267364923000018>. Acesso em 13 jun. 2024.

e aprendizagem de máquina.²⁰

Além disso, a própria dinâmica de constante volatilidade e busca por personalização da experiência do usuário nas plataformas digitais dificulta, e por vezes inviabiliza, identificar se e quando esta prática teria sido aplicada ao conteúdo de algum usuário.²¹

Estratégias de visibilidade do conteúdo digital, a exemplo do *shadowbanning*, são aplicadas de formas variadas²²: o conteúdo alvo pode tornar-se “invisível” ou apenas ter o seu alcance reduzido²³. As restrições de visibilidade são sutis, personalizáveis, podendo incidir sobre determinados grupos de usuários ou ainda sobre certas regiões demográficas²⁴ ou também por conta de mudanças estruturais nos métodos de ranqueamento das plataformas.

Deste modo, as plataformas digitais projetam-se cada vez mais como modeladoras das estruturas tecnológicas, de mercado, das relações entre seus usuários, bem como da gestão da informação e do debate de questões afetas ao público geral.²⁵

20. LEERSEN, Paddy. The Soap Box as a Black Box: Regulating Transparency in Social Media Recommender Systems. *European Journal of Law and Technology*, v. 11, n. 2, mar. 2020. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3544009. Acesso em 13 jun. 2024.

21. JAIDKA, Kokil; MUKERJEE, Subhayan; LELKES, Yphtach. Silenced on social media: The gate-keeping functions of shadowbans in the American Twitterverse. *Journal of Communication*, abr. 2022. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4087843. Acesso em 13 jun. 2024.

22. GILLESPIE, Tarleton. Do Not Recommend? Reduction as a Form of Content Moderation. *Social Media + Society*. v. 8, i. 3, jul.-set. 2022. Disponível em: <https://journals.sagepub.com/doi/full/10.1177/20563051221117552>. Acesso em 13 jun. 2024.

23. JAIDKA, Kokil; MUKERJEE, Subhayan; LELKES, Yphtach. Silenced on social media: The gate-keeping functions of shadowbans in the American Twitterverse. *Journal of Communication*, abr. 2022. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4087843. Acesso em 13 jun. 2024.

24. FLYVERBOM, Mikkel. *The Digital Prism: Transparency and managed visibilities in a datafied world*. New York: Cambridge University Press, 2019.

25. MULLIGAN, Deirdre, K.; BAMBERGER, Kenneth A. Allocating Responsibility in Content Moderation: A Functional Framework. *Berkeley Technology Law Journal*. Berkeley: University of California School of Law. v. 36, n. 03, p. 1091-1171, 2021. p. 1095.; STRANGE, Susan. *States and markets: An introduction to International Political Economy*. London: Pinter Publishers, 1993. Disponível em:

Paralelamente, os agentes privados, responsáveis pela administração das plataformas digitais, exercem um crescente poder normativo-regulador que se consolida, sobretudo, por meio de instrumentos contratuais, como termos de uso e padronizações de natureza técnica²⁶ com o auxílio de tecnologias algorítmicas e inteligências artificiais.²⁷

Nesse sentido, a avaliação, a curadoria e a seleção dos conteúdos veiculados no meio digital também são cada vez mais operadas por estas tecnologias²⁸. Entretanto, as métricas, os critérios e as etapas da moderação de conteúdo ainda são desconhecidas pelo público em geral e pelos usuários destas plataformas²⁹, denotando o problema da transparência e do acesso às informações sobre a operação e os critérios utilizados, inclusive, na prática do *shadowbanning*.

Diante deste cenário, diferentes estudos e esforços regulatórios interdisciplinares são empreendidos, com diversos enfoques, na tentativa de compreender melhor o funcionamento do *shadowbanning*, bem como desenvolver estratégias para o regramento desta prática e de seus potenciais riscos.

Deste modo, o presente estudo busca compreender como esta prática é abordada sob a perspectiva jurídico-regulatória. Há instrumentos legais suficientes para o regramento do *shadowbanning* e para assegurar ao público em geral o direito à

http://www.adelinotorres.info/desenvolvimento/SUSAN%20STRANGE_States%20and%20Markets_%20Susan%20Strange.pdf. Acesso em 14 jun. 2024.

26. BELL, Luca; FRANCISCO, Pedro Augusto P.; ZINGALES, Nicolo, Law of the Land or Law of the Platform? Beware of the Privatisation of Regulation and Police. In: BELL, Luca; ZINGALES, Nicolo (Orgs.). *Platform regulations: how platforms are regulated and how they regulate us*. Rio de Janeiro: FGV Direito Rio, 2017, p. 41–64. Disponível em: <https://repositorio.fgv.br/items/3beee3bb-fb8f-4648-b7da-aa97fc354052>. Acesso em 14 jun. 2024.
27. OLIVA, Thiago D. Content Moderation Technologies: Applying Human Rights Standards to Protect Freedom of Expression. *Human Rights Law Review*, 20, p. 607–640, 2020. p. 609. Disponível em: <https://academic.oup.com/hrlr/article/20/4/607/6023108>. Acesso em 14 jun. 2024.
28. GILLESPIE, Tarleton. The Relevance of Algorithms. In: GILLESPIE, Tarleton; BOCZKOWSKI, Pablo; FOOT, Kirsten. *Media Technologies: Essays on Communication, Materiality, and Society*. Cambridge, MA: MIT Press. Disponível em: <https://www.semanticscholar.org/paper/The-Relevance-of-Algorithms-Gillespie-Boczkowski/746fe3c376041dbd1a5a042584f47bff02c0d272>. Acesso em 14 jun. 2024.

29. PASQUALE, Frank. *The black box society*. Harvard University Press, 2015.

informação e à transparência quanto à gestão das plataformas digitais sobre os conteúdos publicados por seus usuários?

Estas são as questões que se buscará responder na próxima seção deste estudo.

3. ASPECTOS REGULATÓRIOS DO SHADOWBANNING: OBSERVAÇÃO NORMATIVA A PARTIR DO DIGITAL SERVICES ACT (DSA) E DO MARCO CIVIL DA INTERNET

3.1 Digital Services Act (DSA)

Entre diferentes aspectos peculiares, a diretiva do *Digital Services Act* (DSA) se destaca por introduzir, de forma mais concreta, deveres proporcionais às plataformas online de grande porte³⁰, incluindo regras de moderação de conteúdo digital. Além disso, esta diretiva foi pioneira ao abordar especificamente o tema do *shadowbanning*.

Esta diretiva prevê a inclusão de pessoal humano capacitado para avaliar e supervisionar os possíveis impactos gerados pela tomada de decisões automatizadas e para analisar o contexto em que a moderação de conteúdo é aplicada, conforme se observa no Considerando 87.³¹

Sobre a moderação de conteúdo digital, o DSA introduziu os elementos gerais da estrutura denominada *notice-and-action*, em que as plataformas serão responsabilizadas por eventuais conteúdos ilícitos ou indevidos apenas quando faltarem com o

30. BUENO, Thales M.; CANAAN, Renan G. The Brussels Effect in Brazil: Analyzing the impact of the EU digital services act on the discussion surrounding the fake news bill. *Telecommunications Policy*, 48, p. 1-15, 2024. p. 5. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0308596124000545#sec4>. Acesso em 29 jun. 2024.

31. “(...) Outras medidas adequadas podem incluir a adaptação dos seus sistemas de moderação de conteúdos e processos internos ou a adaptação dos seus processos e recursos de tomada de decisão, nomeadamente no que respeita ao pessoal responsável pela moderação de conteúdos e à sua formação e conhecimentos especializados a nível local. (...)” (EUROPEAN UNION. Digital Services Act. *REGULATION (EU) 2022/2065 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)*. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065>. Acesso em 13 jun. 2024).

seu dever de notificar a pessoa ou a entidade que possa sofrer prejuízos decorrentes de um conteúdo ilegal. Por meio do *notice-and-action*, busca-se, entre outros objetivos, evitar com que os prestadores de serviços digitais realizem uma censura prévia dos conteúdos postados por seus usuários.

Para tanto, a diretiva europeia reforça o dever de informação que as plataformas possuem em relação aos seus usuários, como previsto nos artigos 14³² e 17³³. Logo, os prestadores de serviços digitais deverão incluir, nos termos e condições de suas plataformas, informações sobre eventuais restrições que impuserem sobre o uso de seus serviços, bem como sobre as políticas, medidas, procedimentos e ferramentas utilizadas no mecanismo de moderação de conteúdos, seja esta moderação de origem algorítmica ou humana.

-
32. “Art.14: Os prestadores de serviços intermediários devem incluir nos seus termos e condições informações sobre quaisquer restrições que imponham em relação à utilização do seu serviço no que diz respeito às informações prestadas pelos destinatários do serviço. Essas informações incluem informações sobre quaisquer políticas, procedimentos, medidas e instrumentos utilizados para efeitos de moderação de conteúdos, incluindo a tomada de decisões algorítmicas e a análise humana, bem como as regras processuais do respectivo sistema interno de gestão de reclamações. Devem ser apresentadas em linguagem clara, simples, inteligível, facilmente compreensível e inequívoca, e disponibilizadas ao público num formato facilmente acessível e legível por máquina.” (EUROPEAN UNION. Digital Services Act. *REGULATION (EU) 2022/2065 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC* (Digital Services Act). Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065>. Acesso em 13 jun. 2024).
33. “Art. 17: 1. Os prestadores de serviços de alojamento virtual devem apresentar uma exposição de motivos clara e específica a todos os destinatários do serviço afetados relativamente a qualquer uma das seguintes restrições impostas com o fundamento de que as informações fornecidas pelo destinatário do serviço constituem conteúdo ilegal ou são incompatíveis com os seus termos e condições: a) Quaisquer restrições à visibilidade de elementos específicos de informação fornecidos pelo destinatário do serviço, nomeadamente a supressão de conteúdos, a desativação do acesso a conteúdos ou a despromoção de conteúdos; b) Suspensão, cessação ou outra restrição dos pagamentos monetários; c) Suspensão ou cessação da prestação do serviço, no todo ou em parte; d) Suspensão ou encerramento da conta do destinatário do serviço.” (EUROPEAN UNION. Digital Services Act. *REGULATION (EU) 2022/2065 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC* (Digital Services Act). Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065>. Acesso em 13 jun. 2024).

O artigo 14 (4) acrescenta que estes prestadores de serviço deverão agir diligentemente, em observância aos preceitos da liberdade de expressão, do pluralismo dos meios de comunicação social e de outras garantias fundamentais.

Todavia, apesar do DSA contemplar as garantias da liberdade de expressão, da transparência e da explicabilidade ao usuário, esta diretiva não estabeleceu as balizas sobre como deve ser o procedimento da moderação de conteúdo em si e nem sobre a atuação das plataformas no uso de sistemas automatizados para tal moderação.³⁴

Já com relação ao *shadowbanning*, o Considerando 55 do DSA prevê que sua prática consiste na “despromoção nos sistemas de classificação ou de recomendação, bem como na limitação da acessibilidade de um ou mais destinatários do serviço ou no bloqueio do utilizador de uma comunidade em linha sem que o mesmo disso tenha conhecimento”.³⁵

De acordo com o art. 17 do DSA, na hipótese de conteúdo ilegal³⁶ ou incompatível com os termos e condições das plataformas, pode-se aplicar o *shadowbanning* por meio de: “a) quaisquer restrições à visibilidade de elementos específicos de informação fornecidos pelo destinatário do serviço, nomeadamente a supressão de conteúdos, a desativação do acesso a conteúdos ou a despromoção de conteúdos; b) Suspensão, cessação ou outra restrição dos pagamentos monetários; c) Suspensão ou

34. ENARSSON, Therese. Online Content Moderation in and Beyond the EU Digital Services Act – Exploring the Tension between Automated Speed and Human Contextuality. SSRN, abr. 2024. p. 9. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4806704. Acesso em 15 jun. 2024.

35. EUROPEAN UNION. Digital Services Act. *REGULATION (EU) 2022/2065 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC* (Digital Services Act). Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065>. Acesso em 13 jun. 2024.

36. O art. 17 (5) do DSA traz a ressalva da inaplicabilidade do art. 17 às decisões previstas no art. 9º (atuação das plataformas após notificação de autoridades judiciárias ou administrativas da União Europeia sobre conteúdos ilegais) (EUROPEAN UNION. Digital Services Act. *REGULATION (EU) 2022/2065 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC* (Digital Services Act). Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065>. Acesso em 13 jun. 2024).

cessação da prestação do serviço, no todo ou em parte (...)”.³⁷

Ainda sobre estas aplicações de *shadowbanning*, o DSA traz a ressalva de que cabe às plataformas apresentar aos afetados os motivos da aplicação destas restrições, de forma clara e específica.³⁸

Tal exposição de motivos deve indicar qual restrição foi aplicada (supressão, desativação do acesso às informações, despromoção ou restrição da visibilidade das informações), bem como apontar os fatos e as circunstâncias que motivaram a imposição da restrição ao usuário, além das informações sobre o uso de mecanismos automatizados; menção ao fundamento jurídico, quando se tratar de conteúdos ilegais; referência à cláusula contratual eventualmente violada. Também devem haver informações sobre mecanismos internos de resolução extrajudicial de conflitos e vias judiciais para que o usuário possa reclamar ou apresentar recurso contra a medida de *shadowbanning*.³⁹

Além disso, o art. 27 da diretiva europeia prevê a necessidade de transparência sobre os sistemas de recomendação das plataformas digitais, cujos termos e condições devem apresentar, de forma clara, os principais parâmetros utilizados, além da disponibilização de opções para que os destinatários dos serviços possam alterar ou influenciar tais parâmetros.⁴⁰

37. EUROPEAN UNION. Digital Services Act. *REGULATION (EU) 2022/2065 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC* (Digital Services Act). Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065>. Acesso em 13 jun. 2024.

38. EUROPEAN UNION. Digital Services Act. *REGULATION (EU) 2022/2065 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC* (Digital Services Act). Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065>. Acesso em 13 jun. 2024.

39. EUROPEAN UNION. Digital Services Act. *REGULATION (EU) 2022/2065 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC* (Digital Services Act). Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065>. Acesso em 13 jun. 2024.

40. EUROPEAN UNION. Digital Services Act. *REGULATION (EU) 2022/2065 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC* (Digital Services Act). Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065>. Acesso em 13 jun. 2024.

Por fim, o artigo 27 estipula que devem ser apresentados aos usuários as seguintes informações: “a) *Os critérios mais significativos para determinar as informações sugeridas ao destinatário do serviço; [e] b) Os motivos da importância relativa destes parâmetros*”.⁴¹

3.2 Marco Civil da Internet (MCI):

Em linhas gerais, a proposta incutida no Marco Civil da Internet conferia ênfase à prevenção da censura, à promoção da liberdade de expressão no espaço online e à responsabilização civil dos provedores de internet.⁴²

O MCI é um importante dispositivo de lei nacional por ter sido o primeiro que, no Brasil, buscou discutir os limites seguros da internet e construir um conjunto de direitos e liberdades civis que expressassem os valores já consagrados pela Constituição Federal de 1988, além de ter adotado um amplo e democrático processo deliberatório que incluiu diversos atores.⁴³⁻⁴⁴

-
41. EUROPEAN UNION. Digital Services Act. *REGULATION (EU) 2022/2065 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC* (Digital Services Act). Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065>. Acesso em 13 jun. 2024.
 42. TOMASEVICIUS FILHO, Eduardo. Marco Civil da Internet: uma lei sem conteúdo normativo. *Estudos Avançados*. São Paulo: Direito GV, v. 30, n. 86, p. 269-285, abr. 2016. p. 273.
 43. LEMOS, Ronaldo. O Marco Civil como símbolo do desejo por inovação no Brasil. In: LEITE, George S.; LEMOS, Ronaldo (Coords.). *Marco Civil da Internet*. São Paulo: Atlas, 2014. p. 4-5.
 44. Por outro lado, além dos pontos positivos do MCI, críticas também podem ser feitas a este dispositivo de lei. Conforme apontado pelo professor Eduardo Tomasevicius, a deliberação do MCI firmou-se na crença equivocada de que as demais leis já existentes no Brasil, como Código Civil, Código Penal e Lei n.9.296/96 (Lei sobre interceptação de comunicações) não teriam aplicação sobre os vínculos jurídicos estabelecidos na internet, quando, na verdade, todas essas legislações podem e devem ser aplicadas ao ambiente virtual. Ainda de acordo com Tomasevicius, outro ponto crítico do MCI diz respeito à certa ingenuidade do legislador brasileiro que, à época, buscou solucionar os problemas extraterritoriais da internet por meio de uma legislação de alcance apenas nacional. Por fim, o professor aponta uma terceira questão sensível do MCI: prever sobre a neutralidade da rede, sem que se soubesse, no momento deliberativo desta lei, quais seriam os responsáveis pelo financiamento da qualidade do tráfego da internet e sem que houvesse esta mesma previsão legal por parte dos outros países também inseridos na rede mundial da internet

Com o passar dos anos, as novas implicações propiciadas pela internet e a sofisticação das tecnologias digitais, passou-se a compreender que a liberdade de expressão era apenas uma das facetas de um complexo maior de desafios e direitos fundamentais.⁴⁵

Deste modo, o mote do MCI firmou-se na busca pela promoção de direitos sem perder de vista o contexto fático e a devida atenção às diretrizes da proporcionalidade, adequação e necessidade, com o intuito de desenvolver um ambiente digital que impulsionasse a inovação, o desenvolvimento econômico e a tutela aos usuários e demais interessados nas plataformas digitais.⁴⁶

Sendo assim, além da liberdade de expressão, preceito caro ao MCI⁴⁷, este

(TOMASEVICIUS FILHO, Eduardo. Marco Civil da Internet: uma lei sem conteúdo normativo. *Estudos Avançados*. São Paulo: Direito GV, v. 30, n. 86, p. 269-285, abr. 2016. p. 276-277).

45. DIAS, Daniel; BELLI, Luca; ZINGALES, Nicolo; GASPAR, Walter B.; CURZI, Yasmin. Plataformas no Marco Civil da Internet: a necessidade de uma responsabilidade progressiva baseada em riscos. *Civilistica.com*, a. 12. n. 3. 2023. Disponível em: <https://civilistica.emnuvens.com.br/redc/article/view/931/737>. p. 7. Acesso em 14 jun. 2024.
46. DIAS, Daniel; BELLI, Luca; ZINGALES, Nicolo; GASPAR, Walter B.; CURZI, Yasmin. Plataformas no Marco Civil da Internet: a necessidade de uma responsabilidade progressiva baseada em riscos. *Civilistica.com*, a. 12. n. 3. 2023. Disponível em: <https://civilistica.emnuvens.com.br/redc/article/view/931/737>. p. 8. Acesso em 14 jun. 2024.
47. Conforme elucidado por Chiara de Teffé e Carlos Affonso Souza: “A missão da Lei [MCI] foi a de encontrar um equilíbrio entre a criação de um espaço onde fosse possível cultivar as liberdades de expressão e de informação e, ao mesmo tempo, garantir à vítima da disponibilização de conteúdo lesivo os meios adequados para identificar seu ofensor e para remover o material impugnado. De um lado, o MCI retira do provedor a pressão de remover todo e qualquer conteúdo apontado como ilícito, o que atingiria em cheio a liberdade de expressão, mas, de outro, não impede que assim ele proceda caso entenda que o material questionado é realmente contrário aos termos de uso e demais políticas que regem o funcionamento de sua plataforma” (TEFFÉ, Chiara Spadaccini de; SOUZA, Carlos Affonso. Responsabilidade civil de provedores na rede: análise da aplicação do marco civil da internet pelo Superior Tribunal de Justiça. *Revista IBERC*, v.1, n. 1, nov.-fev./2019. p. 09. Disponível em: <https://revistaiberc.responsabilidadecivil.org/iberc/article/view/6/5>. Acesso em 14 jun. 2024). No mesmo sentido seguem Daniel Dias, Luca Belli e outros (DIAS, Daniel; BELLI, Luca; ZINGALES, Nicolo; GASPAR, Walter B.; CURZI, Yasmin. Plataformas no Marco Civil da Internet: a necessidade de uma responsabilidade progressiva baseada em riscos. *Civilistica.com*, a. 12. n. 3. 2023. Disponível em: <https://civilistica.emnuvens.com.br/redc/article/view/931/737>. p. 5. Acesso em 14 jun. 2024).

dispositivo de lei tem também outros fundamentos, como abertura, pluralidade, livre iniciativa, livre concorrência, defesa do consumidor, finalidade social da rede, entre outros.⁴⁸

Some-se os seus princípios, como as garantias da comunicação e manifestação do pensamento, neutralidade de rede, liberdade dos modelos de negócios, promoção da inovação e adesão aos padrões tecnológicos abertos que propiciem a acessibilidade e a interoperabilidade entre as aplicações e as bases de dados.⁴⁹

Ainda, o MCI busca assegurar os usuários no meio digital com diversas garantias, a exemplo do direito de obter “*informações claras e completas constantes dos contratos de prestação de serviços, (...) bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade*”, conforme disposto no art. 7º, VI.⁵⁰

Já com relação à moderação de conteúdo nas plataformas digitais, as normas do Marco Civil da Internet buscam evitar abusos e filtragens injustificadas por parte das plataformas digitais, além de assegurar o contraditório e a ampla defesa às partes envolvidas. Além disso, o MCI permite que os provedores de aplicações estipulem critérios para esta moderação e para a remoção direta de conteúdo, por meio de seus termos e políticas de uso⁵¹.

Nesta linha, o art. 19 estabelece que o provedor de aplicações de internet apenas

48. BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. *Diário Oficial da União*: Brasília, DF, 23 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 14 jun. 2024.

49. BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. *Diário Oficial da União*: Brasília, DF, 23 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 14 jun. 2024.

50. BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. *Diário Oficial da União*: Brasília, DF, 23 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 14 jun. 2024.

51. TEFFÉ, Chiara Spadaccini de; SOUZA, Carlos Affonso. Responsabilidade civil de provedores na rede: análise da aplicação do marco civil da internet pelo Superior Tribunal de Justiça. *Revista IBERC*, v.1, n. 1, nov.-fev./2019. Disponível em: <https://revistaiberc.responsabilidadecivil.org/iber/article/view/6/5>. Acesso em 14 jun. 2024.

terá a obrigação legal de remover determinado conteúdo mediante ordem judicial específica, no âmbito e conforme os limites técnicos de seu serviço.^{52 53}

Por outro lado, considerando a crescente sofisticação das tecnologias utilizadas na moderação de conteúdo e as diferentes formas de se moderar, a lógica binária prevista no art. 19 do MCI (remover ou não remover o conteúdo)⁵⁴ parece não conseguir conferir amplo tratamento jurídico às questões mais atuais da moderação⁵⁵ e nem às suas formas intermediárias, como o *shadowbanning*.

Feitas estas considerações iniciais, quais seriam, então, as principais ferramentas do sistema normativo brasileiro para lidar com o *shadowbanning* e os seus possíveis efeitos? A discussão do tema será desenvolvida na seção seguinte deste trabalho.

4. CÓDIGO CIVIL, CÓDIGO DE DEFESA DO CONSUMIDOR E LEI GERAL

52. BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. *Diário Oficial da União*: Brasília, DF, 23 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 14 jun. 2024.

53. A exceção à regra do art. 19 encontra-se prevista no art. 21 do MCI: “Art. 21. O provedor de aplicações de internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo.” (BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. *Diário Oficial da União*: Brasília, DF, 23 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 14 jun. 2024).

54. Se aplicada de forma equivocada, a medida de remoção do conteúdo pode impactar de forma significativa e até causar danos importantes, como a retirada de dados e fatos elucidativos de momentos históricos ou informações de saúde pública, por exemplo (GOLDMAN, Eric. Content Moderation Remedies. *Michigan Technology Law Review*, v. 28, n.1, 2021. p. 21. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3810580. Acesso em 14 jun. 2024).

55. DIAS, Daniel; BELLI, Luca; ZINGALES, Nicolo; GASPAR, Walter B.; CURZI, Yasmin. Plataformas no Marco Civil da Internet: a necessidade de uma responsabilidade progressiva baseada em riscos. *Civilistica.com*, a. 12. n. 3. 2023. Disponível em: <https://civilistica.emnuvens.com.br/redc/article/view/931/737>. p. 9. Acesso em 14 jun. 2024.

DE PROTEÇÃO DE DADOS COMO POSSÍVEIS FUNDAMENTOS JURÍDICOS PARA A ABORDAGEM DO SHADOWBANNING: PRÓS E CONTRAS

4.1 Código Civil e a teoria do abuso de direito

A relação dos usuários com as plataformas digitais, bem como as práticas de moderação de conteúdo nestas plataformas, são regidas, sobretudo, pelos termos de uso e pelas políticas desenvolvidas por tais plataformas, em um formato jurídico semelhante ao do contrato por adesão.

Em linhas gerais, esta modalidade contratual pode ser compreendida como o pacto cujas cláusulas são elaboradas de antemão por uma das partes, descartada a possibilidade de sua discussão ou negociação dos termos substanciais pelo aderente.^{56 57}

Com relação à moderação de conteúdo digital, em que pese a sua previsão, bem como de alguns de seus critérios, nos termos de uso das plataformas, por outro lado, a prática do *shadowbanning* em si não costuma ser apresentada de forma expressa e clara em tais documentos.

Com isso, os usuários alvos desta prática experimentam a redução da visibilidade e do alcance de suas postagens, o que culmina também na redução de suas oportunidades de interações sociais, profissionais e até mesmo econômicas nas plataformas, tendo em vista que estas redes têm sido cada vez mais utilizadas para diversos fins que extrapolam o mero entretenimento.

Deste modo, ao avaliar e filtrar os conteúdos publicados pelos usuários, reduzindo-lhes a visibilidade e o alcance, sem que estes usuários sejam informados sobre essa prática, podendo causar-lhes diferentes danos, estariam as plataformas digitais abusando de seu direito de moderar os conteúdos?

Para responder a esta pergunta, é preciso antes compreender melhor a teoria

56. GOMES, Orlando. *Contratos de adesão: condições gerais dos contratos*, São Paulo: Revista dos Tribunais, 1972. p. 10.

57. LONGONI KLEE, Antonia E. O conceito de estabelecimento empresarial virtual e a proteção do consumidor nos contratos eletrônicos: algumas reflexões. In: MARTINS, Guilherme Magalhães (Coord.). *Direito Privado e Internet*. São Paulo: Atlas, 2014. p. 206.

jurídica do abuso de direito. Conforme Giuseppe Lumia, abusa de seu direito o indivíduo que exerce sua posição jurídica legítima de forma anormal, ultrapassando os limites da boa fé e da lealdade e perturbando a convivência social e civilmente organizada.⁵⁸

Portanto, o abuso de direito evidencia-se pelo “*exercício de um direito que, muito embora inicialmente amparado pelo ordenamento jurídico, excede manifestamente os limites estabelecidos pelas regras de convivência em sociedade, transgredindo seus fins econômicos ou sociais (...)*”.⁵⁹

Também, António Menezes Cordeiro explica que o abuso de direito está relacionado ao “exercício disfuncional de posições jurídicas”, que se traduz em uma conduta manifestamente excessiva por parte do titular de um direito. Trata-se de um comportamento que ultrapassa os parâmetros do bom senso e da legitimidade jurídica e coletiva e que acaba culminando em consequências sociais, econômicas e jurídicas negativas para outra(s) pessoa(s).⁶⁰

No mesmo sentido segue o Código Civil, cujo art. 187 dispõe que “*também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes*”.^{61 62}

58. LUMIA, Giuseppe. *Teoria da relação jurídica: Lineamenti di teoria e ideologia del diritto*, 3. ed., Milano: Giuffrè, trad. Alcides Tomasetti Jr., 1981. p. 102-23.

59. DANTAS, Paulo R. F. *A proteção contra cláusulas abusivas no Código Civil*, São Paulo: Atlas, 2007. p. 174.

60. CORDEIRO, António. M. Do abuso do direito: estado das questões e perspectivas. *Revista da Ordem dos Advogados*, v. II, a. 65, set. 2005. p. 2; 25. Disponível em: <https://portal.oa.pt/publicacoes/revista-da-ordem-dos-advogados/ano-2005/ano-65-vol-ii-set-2005/artigos-doutrinais/antonio-menezes-cordeiro-do-abuso-do-direito-estado-das-questoes-e-perspectivas-star/#:~:text=%C3%89%20ileg%C3%ADtimo%20o%20exerc%C3%ADcio%20de,social%20ou%20econ%C3%B3mico%20desse%20direito>. Acesso em 26 jun. 2024.

61. BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. *Diário Oficial da União*: Brasília, DF, 10 jan. 2002.

62. O Código Civil também prevê outras hipóteses de exercício irregular do direito, a exemplo dos seguintes dispositivos: “Art. 570. Se o locatário empregar a coisa em uso diverso do ajustado, ou do a que se destina, ou se ela se danificar por abuso do locatário, poderá o locador, além de rescindir o contrato, exigir perdas e danos.”; “Art. 670. Pelas somas que devia entregar ao mandante

Assim, o abuso de direito é uma previsão legal expressa em forma de cláusula geral, o que permite a este dispositivo de lei abarcar as formulações mais genéricas possíveis e contemplar um amplo escopo de situações fáticas. Em razão deste caráter genérico, a verificação judicial de eventual abuso de direito deve se dar não pela via da abstração normativa, mas pela análise das circunstâncias de cada caso concreto.⁶³

Esta espécie de abuso pode materializar-se de três formas diferentes: a) ação ou omissão com o objetivo de gerar prejuízos a alguém; b) conduta que, apesar de não ter o dolo do prejuízo, é desvantajosa para um terceiro e c) comportamento que aparenta oferecer as mesmas utilidades e vantagens às partes envolvidas, mas que na realidade distancia-se do sistema conceitual e valorativo previsto no Código Civil.⁶⁴

Assim, a teoria do abuso de direito busca prevenir condutas que extrapolam o legítimo direito do agente, de modo que, nas relações privadas, haja equilíbrio entre a autonomia da vontade das partes e as vantagens e (eventuais) desvantagens dos envolvidos.

Feitas estas breves considerações sobre a teoria do abuso de direito, retoma-se a pergunta feita anteriormente nesta seção: ao avaliar e filtrar os conteúdos publicados pelos usuários, reduzindo-lhes a visibilidade e o alcance, sem que estes usuários sejam informados sobre essa prática, podendo causar-lhes diferentes danos, estariam as plataformas digitais abusando de seu direito de moderar os conteúdos?

A título ilustrativo e exemplificativo, na subseção seguinte, esta pergunta será

ou recebeu para despesa, mas empregou em proveito seu, pagará o mandatário juros, desde o momento em que abusou.”; “Art. 939. O credor que demandar o devedor antes de vencida a dívida, fora dos casos em que a lei o permita, ficará obrigado a esperar o tempo que faltava para o vencimento, a descontar os juros correspondentes, embora estipulados, e a pagar as custas em dobro.” (BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. *Diário Oficial da União*: Brasília, DF, 10 jan. 2002).

63. CATALAN, Marcos. Primeiras reflexões sobre o abuso de direito nas relações familiares. *IB-DFAM: VI Congresso Brasileiro de Direito de Família*, nov. 2007. p.2. Disponível em: https://ibdfam.org.br/_img/congressos/anais/106.pdf. Acesso em 25 jun. 2024.

64. LAUTENSCHLÄGER, Milton F. A. C. Abuso de direito. *Enciclopédia Jurídica da PUC SP*. Tomo Direito Civil, ed. 1, dez. 2021. p. 6. Disponível em: <https://enciclopediajuridica.pucsp.br/ver-bete/478/edicao-1/abuso-de-direito#:~:text=O%20C%C3%B3digo%20Civil%20de%202002,f%C3%A9%20ou%20pelos%20bons%20costumes%E2%80%9D>. Acesso em 25 jun. 2024.

discutida a partir de um caso concreto decidido pelo Tribunal de Justiça de São Paulo.

4.1.1 *Shadowbanning* nas plataformas digitais: O caso Marcela Balandez x Facebook

O caso em comento chegou à primeira instância do Tribunal de Justiça de São Paulo, em 2023, por meio da ação de obrigação de fazer, ajuizada por Marcela Balandez, em face da empresa Facebook Serviços Online do Brasil LTDA.⁶⁵

De acordo com Balandez, a rede social do Instagram teria desativado diversas funcionalidades de sua conta, incluindo seu alcance e sua “capacidade de engajamento”, sem lhe comunicar previamente e nem lhe conferir oportunidade de defesa. A autora relatou ainda que, à época, fez contato com a empresa, para tratar do assunto, e que a ré restabeleceu o seu perfil, mas, aproximadamente um mês depois, o desativou novamente.

Em sua peça inicial, Balandez alegou também que esta conduta da empresa ré teria reduzido o engajamento de sua conta em mais de 90% na plataforma e que esta redução repercutiu de forma significativa sobre os 7 milhões de visualizações que suas postagens alcançavam antes das mencionadas restrições. A autora pleiteou a reativação das funcionalidades de sua conta no Instagram, além do pagamento indenizatório no importe de R\$50.000,00.

Ao contestar, o Facebook alegou que adotou o procedimento correto, sob a justificativa de que Balandez teria violado os Termos de Uso da plataforma em razão de “*discurso de ódio e bullying*”. Em sentença condenatória, nos termos do art. 373, II, do Código de Processo Civil, a magistrada entendeu que, apesar da relação entre as partes ser regida por contrato de voluntária adesão, o Facebook não apresentou, no processo judicial, elementos capazes de confirmar sua alegação genérica de que Balandez teria violado os termos de uso da plataforma; não cientificou a autora da

65. BRASIL. Tribunal de Justiça do Estado de São Paulo. Apelação Cível nº XXXXX-38.2023.8.26.0100, da 34ª Câmara de Direito Privado do Tribunal de Justiça do Estado de São Paulo, São Paulo, SP, 25 de março de 2024. *Lex*: jurisprudência do Tribunal de Justiça do Estado de São Paulo. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-sp/2319355008/inteiro-teor-2319355017>. Acesso em 28 jun. 2024.

mencionada desativação de certas funcionalidades da conta e nem lhe oportunizou o direito de defesa quando da aplicação das restrições.^{66 67}

O caso abordado acima ilustra as controvérsias envolvidas na prática do *shadowbanning* e as suas repercussões negativas experimentadas pela autora da ação judicial. Assim, em cenários como o do referido caso, é possível argumentar que o *shadowbanning* configura abuso de direito por parte das plataformas digitais, nos termos do art. 187 do Código Civil.

Os argumentos capazes de sustentar a hipótese do *shadowbanning* como abuso de direito são o fato de que as plataformas digitais desenvolvem esta prática de forma silenciosa, sem informar aos usuários afetados, sem conferir-lhes a oportunidade de defesa ou de remoção do conteúdo e também pela não disponibilização clara e acessível dos critérios utilizados na aplicação de *shadowbanning*.

Além destas falhas técnicas e operacionais das plataformas digitais, há que se considerar as (significativas) reduções de oportunidades sociais, profissionais e econômicas (monetização) que os usuários podem experimentar em decorrência desta prática, como ocorreu com Marcela Balandez, autora da ação judicial relatada nesta subseção.⁶⁸

Sendo assim, uma vez confirmada a hipótese do *shadowbanning* como abuso de direito, em análise do caso concreto na esfera judicial, restará à plataforma digital reverter as restrições de alcance e visibilidade impostas à conta do usuário e, se

66. “Art. 373. O ônus da prova incumbe: (...) II - ao réu, quanto à existência de fato impeditivo, modificativo ou extintivo do direito do autor.” (BRASIL. Lei nº 13.105, de 16 de março de 2015. Código de Processo Civil. *Diário Oficial da União*: Brasília, DF, 16 mar. 2015).

67. Posteriormente o Facebook interpôs apelação diante da sentença condenatória. A relatora do recurso, Cristina Zucchi, votou pelo provimento parcial do recurso, apenas para reduzir o valor da indenização por dano moral para o montante de R\$15.000,00 (BRASIL. Tribunal de Justiça do Estado de São Paulo. Apelação Cível nº XXXXX-38.2023.8.26.0100, da 34ª Câmara de Direito Privado do Tribunal de Justiça do Estado de São Paulo, São Paulo, SP, 25 de março de 2024. *Lex: jurisprudência do Tribunal de Justiça do Estado de São Paulo*. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-sp/2319355008/inteiro-teor-2319355017>. Acesso em 28 jun. 2024).

68. CHETTY, Raj *et al.* Social capital I: measurement and associations with economic mobility. *Nature*, 608, p. 108-121, 2022. Disponível em: <https://www.nature.com/articles/s41586-022-04996-4>. Acesso em 29 jun. 2024.

cabível, efetuar o pagamento indenizatório por danos eventualmente experimentados pelo titular da conta, conforme determina o art. 927, do Código Civil.⁶⁹

Por fim, em uma perspectiva de diálogo das fontes, é importante acrescentar que, juntamente com a legislação civil, outros dispositivos de lei podem e devem ser mobilizados para tratar do tema, a exemplo da Lei n. 8.078/90 (Código de Defesa do Consumidor - CDC). Inclusive, esta foi a perspectiva adotada no julgamento do mencionado caso *Marcela Balandez x Facebook*, em que se compreendeu que Balandez era também consumidora do serviço oferecido pelo Instagram (Facebook) e que, portanto, as normas do CDC deveriam incidir sobre o caso.⁷⁰

Por sua vez, a aplicação das normas consumeristas sobre a prática de *shadowbanning* será discutida na próxima seção deste trabalho.

4.2 Código de Defesa do Consumidor (CDC): direito de transparência do usuário-consumidor quanto à prática de *shadowbanning*

Conforme exposto nas seções anteriores deste trabalho, a relação entre os usuários e as plataformas digitais é regida, sobretudo, pelos termos de uso e políticas internas das próprias plataformas, o que denota o vínculo contratual entre os envolvidos.

Além deste vínculo contratual civil, é importante considerar que se trata aqui de uma relação consumerista, atraindo, portanto, a competência normativa também do

69. BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. *Diário Oficial da União*: Brasília, DF, 10 jan. 2002.

70. Amparando-se em jurisprudências nacionais, a relatora do julgamento de apelação do caso *Marcela Balandez x Facebook* seguiu o entendimento expresso por estas jurisprudências, no sentido de considerar a vulnerabilidade técnica, jurídica e econômica de Balandez e enquadrá-la na categoria de “consumidora”, conforme preconiza o art. 2º do CDC (BRASIL. Tribunal de Justiça do Estado de São Paulo. Apelação Cível nº XXXXX-38.2023.8.26.0100, da 34ª Câmara de Direito Privado do Tribunal de Justiça do Estado de São Paulo, São Paulo, SP, 25 de março de 2024. *Lex*: jurisprudência do Tribunal de Justiça do Estado de São Paulo. Disponível em: <https://www.jus-brasil.com.br/jurisprudencia/tj-sp/2319355008/inteiro-teor-2319355017>. Acesso em 28 jun. 2024).

Código de Defesa do Consumidor, nos termos de seu capítulo I.⁷¹

Por sua vez, o CDC contempla uma série de direitos e garantias que buscam regular a relação entre os fornecedores/prestadores de serviços e os seus destinatários finais (consumidores) e minimizar os desequilíbrios técnico, econômico e social existentes entre esses sujeitos.⁷²

Referente aos contratos firmados entre essas partes, o CDC também estipula garantias, a exemplo do direito básico do consumidor de receber informações claras e adequadas sobre as características, qualidade, quantidade, riscos, entre outros elementos, dos produtos e serviços contratados, conforme disposto no art. 6º, III deste diploma normativo.⁷³

Outra previsão normativa importante, incluída pelo CDC, é o dever de transparência dos prestadores de serviços no sentido de informar o consumidor a respeito da “*modificação das cláusulas contratuais que estabeleçam prestações desproporcionais ou sua revisão em razão de fatos supervenientes que as tornem excessivamente onerosas*”⁷⁴. O CDC também determina, no art. 54, §4º, que serão nulas, quando não

71. De acordo com os arts. 2º e 3º do CDC, *consumidor* é “toda pessoa física ou jurídica que adquire ou utiliza produto ou serviço como destinatário final” e *fornecedor* se refere a “toda pessoa física ou jurídica, pública ou privada, nacional ou estrangeira, bem como os entes despersonalizados, que desenvolvem atividade de produção, montagem, criação, construção, transformação, importação, exportação, distribuição ou comercialização de produtos ou prestação de serviços” (BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. *Diário Oficial da União*: Brasília, DF, 11 set. 1990).

72. ALMEIDA, Marcos E.; SISTER, Tatiana D.; FALOPPA, Priscila O. Contratos Eletrônicos Interativos e a Relativização do Pacta Sunt Servanda sobre os Termos de Uso das Plataformas Digitais. *PEER REVIEW*, v. 6, nº 5, 2024. p. 87. Disponível em: <https://peerw.org/index.php/journals/article/view/1889/1088>. Acesso em 26 jun. 2024.

73. BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. *Diário Oficial da União*: Brasília, DF, 11 set. 1990. Sobre o tema, vale destacar que o acesso à informação e a vedação da discriminação injusta são garantias já previstas inclusive na Constituição Federal, a exemplo de seu art. 5º, *caput* e inciso XIV (BRASIL. Constituição da República Federativa do Brasil de 1988. Promulgada em 5 de outubro de 1988. *Diário Oficial da União*: Brasília, DF, 5 out. 1988).

74. BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. *Diário Oficial da União*: Brasília, DF, 11 set. 1990.

destacadas, as cláusulas que impliquem restrições aos direitos do consumidor.⁷⁵

Ainda de acordo com a perspectiva de diálogo das fontes normativas, pode-se acrescentar a previsão do art. 7º, VI, do Marco Civil da Internet, que assegura ao usuário da internet e das plataformas digitais o direito a “*informações claras e completas constantes dos contratos de prestação de serviços, (...) bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade*”.⁷⁶

Deste modo, quando se trata das relações de consumo no meio digital, recai sobre os provedores de serviços online o dever de prestar informações aos seus usuários (consumidores) da forma mais simples e transparente possível, considerando ainda que a interpretação das cláusulas contratuais envolvidas deverá ser feita de modo mais favorável ao consumidor (aderente).

Logo, conforme o sistema normativo consumerista brasileiro, com relação ao *shadowbanning*, trata-se de prática que deveria ser informada com clareza ao usuário, o que incluem informações sobre o momento de sua aplicação, além das motivações para tanto, as bases legais e as cláusulas contratuais justificadoras.

Como exemplo que ilustra a questão, foi noticiado pela mídia, em 2019, o caso de *shadowbanning* do TikTok, que estaria segmentando seus usuários com deficiências físicas, autismo, síndrome de Down e pessoas com sobrepeso, na categoria “usuários especiais”, além de limitar o alcance das publicações feitas por esses usuários.⁷⁷

Esta conduta da plataforma, se analisada sob o prisma do CDC, poderia ser enquadrada como um método comercial desleal e como prática abusiva, nos termos do art. 6º, IV⁷⁸, uma vez que, até onde é possível saber, não há motivações que

75. “Art. 54 - § 4º As cláusulas que implicarem limitação de direito do consumidor deverão ser redigidas com destaque, permitindo sua imediata e fácil compreensão.” (BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. *Diário Oficial da União*: Brasília, DF, 11 set. 1990).

76. BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. *Diário Oficial da União*: Brasília, DF, 23 abr. 2014.

77. FERNANDES, Rodrigo. Seis polêmicas do TikTok em 2019. *TechTudo*, dez. 2019. Disponível em: <https://www.techtudo.com.br/noticias/2019/12/seis-polemicas-do-tiktok-em-2019.ghtml>. Acesso em 17 jun. 2024.

78. “Art. 6º São direitos básicos do consumidor: IV - a proteção contra a publicidade enganosa e abusiva, métodos comerciais coercitivos ou desleais, bem como contra práticas e cláusulas abusivas

justifiquem tal discriminação entre os mencionados usuários.

Assim, com base neste dispositivo de lei, seria possível aos usuários afetados pelo *shadowbanning* questionarem-na administrativa ou judicialmente pela via da ação individual ou coletiva, através dos órgãos de proteção ao consumidor, por exemplo.

Por outro lado, uma vez que as plataformas digitais, incluindo redes sociais como TikTok, Instagram e X (Twitter), são também modelos de negócios, há que se considerar a tensão existente entre os deveres de informação e transparência dessas empresas e a tutela jurídica conferida à sua propriedade intelectual e aos seus segredos comerciais. Trata-se de uma delicada ponderação, cuja medida certa, “ideal” é ainda um dos principais desafios às legislações internacionais e nacionais, bem como aos respectivos órgãos reguladores e estudiosos do tema.

Diante deste cenário, outra possibilidade jurídico-normativa brasileira para o enfrentamento complementar da prática do *shadowbanning* seria a Lei n. 13.709/2018, também conhecida como Lei Geral de Proteção de Dados.

4.3 Lei n. 13.709/18 (Lei Geral de Proteção de Dados): direito à transparência e direito à revisão de decisões automatizadas sobre a prática de *shadowbanning*

Ao tratarmos da moderação de conteúdo digital, incluindo o *shadowbanning*, é essencial recordar que estas práticas tornaram-se viáveis, em grande medida, em razão da sofisticação tecnológica do tratamento eletrônico de dados pessoais.⁷⁹

Neste cenário a Lei Geral de Proteção de Dados (LGPD) é um dos principais dispositivos de lei nacional responsável por regular o tratamento de dados que ocorre

ou impostas no fornecimento de produtos e serviços” (BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. *Diário Oficial da União*: Brasília, DF, 11 set. 1990).

79. De acordo com o art. 5º, X, da LGPD, o tratamento eletrônico de dados pessoais refere-se a: “toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;” (BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). *Diário Oficial da União*: Brasília, DF, 14 ago. 2018).

durante a moderação de conteúdo das plataformas digitais.

Além de seu conjunto de regras e direitos, a LGPD também prevê, especialmente no art. 6º, um sistema principiológico cujo papel é nortear e fornecer diretrizes éticas para a adequada interpretação e aplicação de suas normas.⁸⁰

Dentro deste conjunto principiológico destaca-se resumidamente aqui os princípios da *finalidade*, *transparência*, *não discriminação* e *prestação de contas*. O primeiro disciplina que o tratamento de dados pessoais deve servir a propósitos legítimos, específicos e informados ao titular dos dados. Já o segundo (*transparência*) busca assegurar o equilíbrio entre o fornecimento, ao titular, de informações claras, precisas, facilmente compreensíveis sobre tal tratamento, sem perder de vista a adequada proteção aos segredos comerciais e industriais.⁸¹

Ao seu turno, o princípio da *não discriminação* veda o tratamento de dados pessoais para fins discriminatórios ou ilícitos. Por fim, a *prestação de contas* refere-se à “*demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas*”.⁸²

Além do substrato principiológico, a LGPD, no art. 7º, também elenca as diferentes bases legais que autorizam o tratamento de dados pessoais. Para os fins do

80. FRAZÃO, Ana. *A nova Lei Geral de Proteção de Dados Pessoais: principais repercussões para a atividade empresarial*: parte I. 2018. p. 4. Disponível em: https://www.professoraanafracao.com.br/files/publicacoes/2018-08-30-A_nova_Lei_Geral_de_Protecao_de_Dados_Pessoais_Principais_repercussoes_para_a_atividade_empresarial_Parte_I.pdf. Acesso em 27 jun. 2024.

81. Sobre o direito à informação, acrescente-se ainda o art. 9º da LGPD: “O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso: I - finalidade específica do tratamento; II - forma e duração do tratamento, observados os segredos comercial e industrial; III - identificação do controlador; IV - informações de contato do controlador; V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade; VI - responsabilidades dos agentes que realizarão o tratamento; e VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.” (BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). *Diário Oficial da União*: Brasília, DF, 14 ago. 2018).

82. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). *Diário Oficial da União*: Brasília, DF, 14 ago. 2018.

presente estudo, destaca-se aqui a base prevista no inciso V, relacionada à execução de contrato ou aos procedimentos contratuais preliminares⁸³, hipótese em que se enquadram os termos de uso que regem as práticas de moderação de conteúdo das plataformas digitais.

Some-se ao conjunto de princípios e regras a previsão da LGPD sobre os direitos dos titulares dos dados pessoais, com ênfase sobre dois deles: *direito à revisão de decisões automatizadas* (art. 20) e *direito à transparência* (presente em diferentes dispositivos da Lei Geral de Proteção de Dados), abordados aqui em razão de sua associação mais direta às práticas de moderação de conteúdo digital, em que se inclui o *shadowbanning*.

O *direito à revisão de decisões automatizadas* é a prerrogativa que o titular dos dados possui de defender seus próprios interesses quando uma determinada decisão, tomada de forma artificial por sistemas autônomos, afetar os seus aspectos pessoais, profissionais, de crédito, de consumo ou ainda os elementos de sua personalidade.⁸⁴

Já o *direito à transparência*, conforme mencionado anteriormente neste tópico, relaciona-se ao direito à informação, à prestação de contas por parte do agente responsável pelo tratamento dos dados pessoais, de modo a prover preventivamente o titular com informações e subsídios necessários sobre o que é realizado com os seus dados e sobre as medidas que ele pode tomar em caso de abusos ou ilicitudes.

Importante ressaltar que as mencionadas garantias da *revisão de decisões automatizadas* e da *transparência* dialogam entre si, como pode ser observado pela leitura do art. 20, §1º, da LGPD, segundo o qual deverão ser fornecidas “*sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos*

83. “Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados.”. Além desta, há também as bases do consentimento, cumprimento de obrigação legal, proteção da vida ou da incolumidade física do titular, legítimo interesse do controlador, entre outras (BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). *Diário Oficial da União*: Brasília, DF, 14 ago. 2018).

84. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). *Diário Oficial da União*: Brasília, DF, 14 ago. 2018.

*utilizados para a decisão automatizada, observados os segredos comercial e industrial”.*⁸⁵

Por outro lado, a menção deste dispositivo de lei aos segredos comercial e industrial traz o desafio adicional sobre como compatibilizar, na prática, a transparência das decisões automatizadas e o segredo das operações algorítmicas desenvolvidas pelos atores empresariais, a exemplo das plataformas digitais em suas práticas de moderação de conteúdo⁸⁶. Trata-se de questão complexa, que demanda esforços conjuntos e interdisciplinares, para além das disposições dos textos legais.

Todavia, mesmo quando se tratar de segredo comercial ou industrial, o legislador brasileiro buscou apresentar um caminho possível para a viabilização da transparência e da revisão de decisões automatizadas, por meio do art. 20, §2º da LGPD, permitindo com que a respectiva autoridade nacional - Agência Nacional de Proteção de Dados (ANPD), realize auditoria de determinado sistema para verificar possíveis aspectos discriminatórios no tratamento automatizado de dados pessoais⁸⁷. Esta é uma importante previsão legal que pode orientar outras regulamentações mais específicas sobre o tema e contribuir para a operacionalização desta auditoria em termos mais práticos.

Além disso, a título exemplificativo e ilustrativo, é possível não apenas correlacionar as mencionadas disposições da Lei Geral de Proteção de Dados, do Código Civil e do Código de Defesa do Consumidor como também testar, ainda que hipoteticamente, sua aplicação casuística nas práticas de moderação de conteúdo digital, mais especificamente, em relação ao *shadowbanning*.

Para tanto, utilizando o mesmo caso, previamente abordado no tópico 4.2 deste trabalho⁸⁸, identifica-se que o TikTok, além de incorrer na suposta prática de

85. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). *Diário Oficial da União*: Brasília, DF, 14 ago. 2018.

86. FRAZÃO, Ana. *A nova Lei Geral de Proteção de Dados Pessoais: principais repercussões para a atividade empresarial*: parte I. 2018. p. 6. Disponível em: https://www.professoraanafracao.com.br/files/publicacoes/2018-08-30-A_nova_Lei_Geral_de_Protecao_de_Dados_Pessoais_Principais_repercussoes_para_a_atividade_empresarial_Parte_I.pdf. Acesso em 27 jun. 2024.

87. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). *Diário Oficial da União*: Brasília, DF, 14 ago. 2018.

88. O caso, noticiado pela mídia em 2019, trata de suposto *shadowbanning* praticado pelo TikTok,

shadowbanning, utilizou também dados pessoais sensíveis⁸⁹ de saúde dos usuários alvos, tendo em vista tratar-se de pessoas com deficiências físicas, sobrepeso e questões como autismo e síndrome de Down, cujas publicações na plataforma tiveram o alcance reduzido, ao que parece, em razão dessas condições físicas e de saúde.

Este tratamento discriminatório, amparado em dados sensíveis, é vedado pela LGPD, conforme dispõe o art. 11, §1º: “*Aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica.*”.

Na mesma linha segue o art. 21 desta lei, ao assegurar que os dados pessoais não podem ser utilizados em prejuízo de seus titulares quando estes estiverem dentro do exercício regular dos seus direitos.⁹⁰

Além disso, é possível que tal prática do TikTok configure uma modalidade de abuso de direito, nos termos do art. 187, do Código Civil, a partir do momento em que a plataforma extrapola suas prerrogativas contratuais legítimas, ao adotar critérios discriminatórios ilícitos na moderação e curadoria de conteúdo, restringindo as possibilidades de postagens, interações e limitando oportunidades profissionais e econômicas de determinados usuários de sua plataforma.⁹¹

Some-se a isso a falta de transparência sobre os critérios discriminatórios e classificatórios adotados pelo TikTok neste caso, o que desafia, e até mesmo inviabiliza, as garantias consumeristas à informação e ao questionamento desta prática por parte

que estaria segmentando seus usuários com deficiências físicas, autismo, síndrome de Down e pessoas com sobrepeso, na categoria de “usuários especiais” e limitando o alcance das publicações feitas por esses usuários.

89. De acordo com o art. 5º, II, da LGPD, os dados pessoais sensíveis se referem aqueles de: “origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, *dado referente à saúde* ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural” (grifos nossos) (BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). *Diário Oficial da União*: Brasília, DF, 14 ago. 2018).

90. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). *Diário Oficial da União*: Brasília, DF, 14 ago. 2018.

91. BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. *Diário Oficial da União*: Brasília, DF, 10 jan. 2002.

dos usuários envolvidos.

Desta forma, caso a hipótese, de abuso de direito pela plataforma digital, se confirmasse, em sede judicial, entre outras medidas, os usuários afetados fariam jus à reparação civil por danos, conforme dispõe o art. 927 do Código Civil.⁹²

Também, uma vez que estes usuários se enquadram na categoria de consumidores, seria possível aos respectivos órgãos de proteção desta categoria ingressar com uma ação judicial coletiva para questionar e solicitar as medidas adequadas quanto à mencionada prática de *shadowbanning*, de acordo com o art. 81 do CDC.⁹³

Há ainda outros casos de *shadowbanning* em que as disposições do Código Civil, do Código de Defesa do Consumidor e da Lei Geral de Proteção de Dados poderiam ser aplicadas. É o que ocorreu, por exemplo, com determinados usuários da plataforma X (Twitter), que identificaram alterações no alcance e na visibilidade de suas publicações.

O primeiro caso refere-se à conta de Jay Bhattacharya, que leciona sobre políticas em saúde na Universidade de Stanford. Durante a pandemia da Covid-19 o professor publicou, em sua conta no X, que o *lockdown* poderia prejudicar as crianças. Após esta afirmação, sua conta foi movida pela plataforma para a *Trends Blacklist* (*lista negra de tendências*, em uma tradução literal), uma lista que impede que os *tweets* se tornem tendência na rede.⁹⁴

Por sua vez, o influenciador de direita Dan Bongino teve sua conta incluída na *Search Blacklist* (*lista negra de busca*, em uma tradução literal), o que prejudicou os resultados de busca por seu perfil. Já a conta do ativista conservador Charlie Kirk

92. “Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo.” (BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. *Diário Oficial da União*: Brasília, DF, 10 jan. 2002).

93. “Art. 81. A defesa dos interesses e direitos dos consumidores e das vítimas poderá ser exercida em juízo individualmente, ou a título coletivo.” (BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. *Diário Oficial da União*: Brasília, DF, 11 set. 1990).

94. SPAGNUOLO, Sergio. Twitter confirma shadow ban contra certos usuários. *Núcleo*, dez. 2022. Disponível em: <https://nucleo.jor.br/reportagem/2022-12-09-twitter-files-black-lists/>. Acesso em 17 jun. 2024.

recebeu o rótulo *Não* amplificar.⁹⁵

Os três casos versam sobre questões delicadas e controversas, tanto entre os usuários das plataformas digitais quanto nos próprios termos de uso de plataformas como o X (Twitter)⁹⁶. O primeiro caso abordado, referente à conta de Jay Bhattacharya, envolve aspectos e dados sensíveis de saúde coletiva, somados ao período da Covid, além de opiniões divergentes e polêmicas sobre o tema, cujos efeitos extrapolaram a discussão de saúde na pandemia e adquiriram conotação também política, econômica e ideológica.

Por sua vez, o segundo e terceiro casos, de Dan Bongino e Charlie Kirk, também tocam em vieses e pontos político-ideológicos sensíveis, de desafiadora delimitação entre quais conteúdos, por um lado, fomentariam o debate público saudável, equilibrado, permeado pela legítima liberdade de expressão e quais, por outro lado, incitariam posições extremistas, violentas e polarizadas nas plataformas digitais⁹⁷.

Deste modo, os três casos acima abrem margem para diferentes interpretações legais. A depender do contexto e de outras variáveis, pode-se afirmar que os titulares dessas contas teriam atuado em conformidade com o seu direito legítimo de postar e interagir com os demais usuários da plataforma, com fundamento na legislação civil contratual brasileira.

Por outro lado, é possível que esses titulares, em algumas de suas publicações, por incluírem dados sensíveis de saúde e de orientações político-ideológicas, tenham extrapolado os limites do seu direito legítimo, incidindo, hipoteticamente, até em casos de desinformação e outras situações problemáticas.

Consequentemente, há que se considerar que estes elementos constituem desafios adicionais à moderação de conteúdo nas plataformas digitais, sobretudo, aos seus

95. SPAGNUOLO, Sergio. Twitter confirma shadow ban contra certos usuários. *Núcleo*, dez. 2022. Disponível em: <https://nucleo.jor.br/reportagem/2022-12-09-twitter-files-black-lists/>. Acesso em 17 jun. 2024.

96. LEE, Edward. Moderating Content Moderation: A Framework for Nonpartisanship in Online Governance. *American University Law Review*. Washington: Washington College of Law. v. 70, n. 03, p. 913-1060, fev. 2021. p. 1059.

97. DOUEK, Evelyn. *Content Moderation as Systems Thinking*. Harvard Law Review. Cambridge: Harvard University Press. v. 136, n. 02, p. 526-607, dez. 2022. p. 537.

sistemas automatizados, compostos majoritariamente por algoritmos e linguagens matemáticas que, apesar de toda a tecnologia empregada atualmente, ainda estão sujeitos a falhas que poderão repercutir significativamente em sua “compreensão”, categorização e em suas formas de moderar.

Diante destas implicações do *shadowbanning* e da moderação de conteúdo, o legislador brasileiro tem buscado enfrentar essas questões por meio de mais discussões regulatórias, a exemplo do Projeto de Lei n. 2630/2020.

4.4 Projeto de Lei n. 2630/2020 - Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet

A moderação de conteúdo digital e os seus diversos efeitos adquiriram relevância significativa ao ponto de tornarem-se temas mais frequentes nas discussões regulatórias internacionais e nacionais. Exemplo disso é o Projeto de Lei brasileiro n. 2630/2020, de autoria do Senador Alessandro Vieira, do partido *Cidadania/SE*.⁹⁸

O PL, intitulado *Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet*, foi proposto como uma ferramenta normativa para enfrentamento da crescente desinformação, disseminação de *fake news* e disputas acerca do que pode ou não ser considerado liberdade de expressão em um ambiente digital cada vez mais explorado por provedores de redes sociais e serviços de mensageria privada.⁹⁹

98. Importante acrescentar que o PL n. 2630/20 se aplica aos provedores de redes sociais e de serviços de mensageria privada com mais de 2.000.000 (dois milhões) de usuários registrados. Para os provedores de menor porte, com menor número de usuários, o mencionado PL pode servir, mas apenas como parâmetro de boas práticas, conforme previsto no respectivo art. 1º, §1º (BRASIL. *Projeto de lei nº 2630, de 2020*. Institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet. Brasília, DF: Senado Federal, 2020. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2256735>. Acesso em 29 jun. 2024).; TOMAZ, Tales. Brazilian Fake News Bill: Strong Content Moderation Accountability but Limited Hold on Platform Market Power. *Journal of the European Institute for Communication and Culture*, v. 30, i. 2, p. 253-267, 2023. p. 259. Disponível em: <https://www.tandfonline.com/doi/full/10.1080/13183222.2023.2201801>. Acesso em 29 jun. 2024.

99. BUENO, Thales M.; CANAAN, Renan G. The Brussels Effect in Brazil: Analysing the impact of the EU digital services act on the discussion surrounding the fake news bill. *Telecommunications Policy*, 48, p. 1-15, 2024. p. 5. Disponível em:

Como uma das estratégias para assegurar os direitos à informação e à liberdade de expressão, o referido PL inclui, por meio da seção IV, duas regras gerais a serem observadas pelas plataformas digitais na moderação de conteúdo: *disponibilização de mecanismos de recurso e observância do devido processo*.

Assim, na hipótese dos conteúdos ou das contas dos usuários sofrerem denúncia ou aplicação de medida de moderação prevista nos termos de uso da plataforma, o art. 12 deste PL determina que “o usuário deve ser notificado sobre a fundamentação, o processo de análise e a aplicação da medida, assim como sobre os prazos e procedimentos para sua contestação”. Ainda, o §3º do art. 12 do PL 2630/20 acrescenta a garantia do usuário de recorrer no caso de indisponibilização de conteúdos e contas por parte das plataformas.¹⁰⁰

Apesar de abordar o tema da moderação de conteúdo, o PL não trata expressamente da prática de *shadowbanning*. Por outro lado, a seção seguinte do projeto (regras de *transparência*), no art. 13, traz algumas previsões que podem contribuir para esclarecer sobre a procedimentalização da moderação de conteúdo e coibir práticas moderadoras potencialmente abusivas, como o *shadowbanning*.

Entre tais previsões estão a exigência de que as plataformas produzam relatórios trimestrais de transparência, com a respectiva divulgação em seus sítios eletrônicos, no idioma português, e em padrões tecnológicos abertos, para informar sobre os procedimentos e as decisões de tratamento de conteúdos.

Estes relatórios devem conter, por exemplo, os dados referentes a engajamentos com conteúdos identificados como irregulares, incluindo o número de visualizações,

<https://www.sciencedirect.com/science/article/pii/S0308596124000545#sec4>. Acesso em 29 jun. 2024.

100. O art. 12 do PL n. 2630/20 prevê também as hipóteses de dispensa desta notificação: “§2º Os provedores dispensarão a notificação aos usuários se verificarem risco: I – de dano imediato de difícil reparação; II – para a segurança da informação ou do usuário; III – de violação a direitos de crianças e adolescentes; IV – de crimes tipificados na Lei nº 7.716, de 5 de janeiro de 1989; V – de grave comprometimento da usabilidade, integridade ou estabilidade da aplicação.” (BRASIL. *Projeto de lei nº 2630, de 2020*. Institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet. Brasília, DF: Senado Federal, 2020. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2256735>. Acesso em 29 jun. 2024).

compartilhamentos e alcance, bem como a informação sobre o número total de medidas de moderação de contas e de conteúdos, especificando sua justificativa, que pode ser: a) o cumprimento dos termos de uso dos provedores de redes sociais; b) o cumprimento deste PL ou c) o cumprimento de ordem judicial, além da exposição das motivações, da metodologia utilizada e do tipo de medida adotada, conforme dispõe o art. 13, §1º e §2º do PL.

Por sua vez, o §4º pode contribuir para maior transparência do processo de moderação de conteúdo e para a redução de restrições possivelmente indevidas sobre as contas dos usuários (*shadowbanning*), ao prever que se deverá buscar a identificação e a distinção entre os conteúdos que trafegam nas plataformas digitais, de modo a identificar aqueles conteúdos que tenham sido disseminados não por usuários humanos, mas por redes artificiais.¹⁰¹

A partir da leitura do PL 2630/20, entre outras constatações, é possível observar as intenções do legislador de fortalecer as medidas de responsabilidade pública e enfrentar os riscos da moderação de conteúdo através da exigência de padrões mais elevados de transparência a serem praticados pelas plataformas digitais.¹⁰²

Por outro lado, o mencionado PL avança de forma pouco significativa no enfrentamento de outras questões estruturais desafiadoras, como o elevado poder de mercado que ainda se concentra nas mãos das plataformas digitais¹⁰³, a exemplo das abusividades em algumas práticas de moderação de conteúdo como o *shadowbanning*.

-
101. “Art. 13 - §4º: Os relatórios e dados disponibilizados devem apontar a relação entre contas automatizadas não identificadas como tal, contas e disseminação de conteúdos, de modo que seja possível a identificação de redes artificiais de disseminação de conteúdo.” (BRASIL. *Projeto de lei nº 2630, de 2020*. Institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet. Brasília, DF: Senado Federal, 2020. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2256735>. Acesso em 29 jun. 2024).
102. BUENO, Thales M.; CANAAN, Renan G. The Brussels Effect in Brazil: Analyzing the impact of the EU digital services act on the discussion surrounding the fake news bill. *Telecommunications Policy*, 48, p. 1-15, 2024. p. 5. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0308596124000545#sec4>. Acesso em 29 jun. 2024.
103. TOMAZ, Tales. Brazilian Fake News Bill: Strong Content Moderation Accountability but Limited Hold on Platform Market Power. *Journal of the European Institute for Communication and Culture*, v. 30, i. 2, p. 253-267, 2023. p. 264. Disponível em: <https://www.tandfonline.com/doi/full/10.1080/13183222.2023.2201801>. Acesso em 29 jun. 2024.

Portanto, a carência de previsão de medidas efetivas para alterar esta dinâmica de mercado e promover um ambiente concorrencial saudável é uma das lacunas do PL 2630/20.¹⁰⁴

De todo modo, apesar das possíveis e necessárias críticas ao mencionado projeto de lei, há que se reconhecer sua iniciativa de discutir e buscar tratar de forma jurídico-regulatória pautas urgentes e relevantes como o combate à desinformação, transparência e boas práticas na moderação de conteúdo digital.

5. DISCUSSÃO E CONCLUSÃO

Cada vez mais as plataformas digitais desempenham papéis de maior relevância e impactos tecnológico, econômico, político e social. Se antes elas serviam apenas a algumas funções, como entretenimento e prestações de alguns serviços, nos últimos tempos elas tem atuado também como veículos de informação, plataformas para novos modelos negociais e espaços para discussões socialmente relevantes.

Neste cenário as tecnologias algorítmicas, bem como as ferramentas de aprendizagem de máquina e aprendizagem em redes neurais são fortes aliadas das plataformas na realização da moderação do conteúdo veiculado por seus usuários e, mais especificamente, na condução do *shadowbanning*, prática esta controversa e de difícil percepção, pelo usuário, quando de sua ocorrência.

Considerando que a temática necessita de uma abordagem sistêmica, na qual se incluem as regulações e tratamento jurídico-normativo, o presente estudo buscou analisar e compreender como a prática do *shadowbanning* é abordada sob a perspectiva jurídico-regulatória e quais são os aspectos normativos assegurados em relação a este tema, com ênfase na análise das seguintes normativas: *Digital Services Act* (DSA) e Marco Civil da Internet (MCI), por meio de revisão bibliográfica e método documental.

Quanto ao DSA, uma de suas propostas mais relevantes é estimular as plataformas

104. LEÃO, Luciana O. projeto de lei 2630/2020 – Lei das fake news – e o cenário da regulação em mercados digitais no brasil diante do Digital Markets Act: um breve panorama. *IDP: Debates em Administração Pública*, v. 4, n. 3, 137, 2023. p. 23. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/redap/article/view/7620>. Acesso em 29 jun. 2024.

digitais a adotarem sistemas capazes de discernir entre um intento malicioso, como a incitação ao crime de terrorismo, por exemplo, e uma intenção de elucidar/conscientizar o público geral sobre os atos terroristas, no procedimento de análise e moderação dos conteúdos veiculados pelos usuários nestas plataformas¹⁰⁵. Trata-se de uma proposta desafiadora, em especial para os próprios sistemas automatizados, que precisarão aprender a reconhecer nuances e subjetividades que são próprias da comunicação humana.

Além disso, por ser uma diretiva mais recente, de 2022, o DSA está evidentemente mais atualizado quanto ao tema e às diferentes aplicações de *shadowbanning* em relação ao MCI que, por sua vez, aborda de forma geral, e binária, a questão da moderação de conteúdo, com ênfase em conteúdos ilícitos e na responsabilização civil das plataformas de aplicações de internet.

Por outro lado, o DSA pouco esclarece as diretrizes sobre como ou em que extensão os provedores de conteúdo devem conciliar um trabalho sistêmico com as suas estruturas de moderação nas plataformas digitais.¹⁰⁶

Ainda, ao considerar relevante a tomada de decisão de forma contextualizada e a inclusão de pessoal humano capacitado para esta análise, observa-se que o DSA não descartou a necessidade de se implementar a revisão humana nas decisões automatizadas¹⁰⁷. Por sua vez, embora o MCI não estipule expressamente sobre esta revisão/supervisão humana, este diploma normativo brasileiro apresenta um conjunto de princípios, fundamentos e garantias que visam assegurar a proteção da

105. ENARSSON, Therese. Online Content Moderation in and Beyond the EU Digital Services Act – Exploring the Tension between Automated Speed and Human Contextuality. SSRN, abr. 2024. p. 46. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4806704. Acesso em 15 jun. 2024.

106. ENARSSON, Therese. Online Content Moderation in and Beyond the EU Digital Services Act – Exploring the Tension between Automated Speed and Human Contextuality. SSRN, abr. 2024. p. 11. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4806704. Acesso em 15 jun. 2024.

107. ENARSSON, Therese. Online Content Moderation in and Beyond the EU Digital Services Act – Exploring the Tension between Automated Speed and Human Contextuality. SSRN, abr. 2024. p. 11. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4806704. Acesso em 15 jun. 2024.

personalidade humana, a finalidade social e os direitos humanos.¹⁰⁸

Deste modo, é possível observar que, embora contemple expressamente o tema do *shadowbanning* e preveja determinadas regras sobre o assunto, por outro lado, o DSA não disciplinou as diretrizes sobre a procedimentalização desta prática de moderação.

Já o MCI, em que pese prever um conjunto principiológico e normativo de garantias do usuário da internet e das plataformas digitais, ainda adota uma lógica binária em termos de moderação (remover ou não remover o conteúdo). Portanto, há uma lacuna no MCI com relação a outras formas intermediárias de moderação, incluindo o próprio *shadowbanning*.

Por fim, conclui-se que há uma tendência, nas plataformas digitais, de fortalecimento dos contratos (termos de uso) como ferramenta de sistematização e disciplina das diretrizes da moderação de conteúdo¹⁰⁹.

Em resposta a esta tendência, o ordenamento jurídico nacional precisará adotar uma perspectiva ainda mais sistêmica, fomentando o diálogo entre as diferentes fontes normativas, como a Constituição Federal, o Código Civil, Código de Defesa do Consumidor, Lei Geral de Proteção de Dados, Marco Civil da Internet, entre outras normas jurídicas, para fornecer um tratamento jurídico mais robusto ao tema da moderação de conteúdo e às suas variações, como o *shadowbanning*.

REFERÊNCIAS

ALMEIDA, Marcos E.; SISTER, Tatiana D.; FALOPPA, Priscila O. Contratos Eletrônicos Interativos e a Relativização do Pacta Sunt Servanda sobre os Termos de Uso das Plataformas Digitais. *PEER REVIEW*, v. 6, n° 5, 2024. Disponível em: <https://peerw.org/index.php/journals/article/view/1889/1088>. Acesso em 26 jun. 2024.

-
108. BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. *Diário Oficial da União*: Brasília, DF, 23 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 14 jun. 2024.
109. MULLIGAN, Deirde, K.; BAMBERGER, Kenneth A. Allocating Responsibility in Content Moderation: A Functional Framework. *Berkeley Technology Law Journal*. Berkeley: University of California School of Law. v. 36, n. 03, p. 1091-1171, 2021. p.1170.

- BAMMAN, David; O'CONNOR, Brendan; SMITH, Noah A. Censorship and Deletion Practices in Chinese Social Media. *First Monday*, 17, 3, mar. 2012. Disponível em: <https://www.semanticscholar.org/paper/Censorship-and-deletion-practices-in-Chinese-social-Bamman-O%27Connor/7c23d25d45b6bf781df6e1975674489604e388e4>. Acesso em 29 jun. 2024.
- BELLI, Luca; FRANCISCO, Pedro Augusto P.; ZINGALES, Nicolo, Law of the Land or Law of the Platform? Beware of the Privatisation of Regulation and Police. In: BELLI, Luca; ZINGALES, Nicolo (Orgs.). *Platform regulations: how platforms are regulated and how they regulate us*. Rio de Janeiro: FGV Direito Rio, 2017, p. 41–64. Disponível em: <https://repositorio.fgv.br/items/3beee3bb-fb8f-4648-b7da-aa97fc354052>. Acesso em 14 jun. 2024.
- BRASIL. Constituição da República Federativa do Brasil de 1988. Promulgada em 5 de outubro de 1988. *Diário Oficial da União*: Brasília, DF, 5 out. 1988.
- BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. *Diário Oficial da União*: Brasília, DF, 11 set. 1990.
- BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. *Diário Oficial da União*: Brasília, DF, 10 jan. 2002.
- BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. *Diário Oficial da União*: Brasília, DF, 23 abr. 2014.
- BRASIL. Lei nº 13.105, de 16 de março de 2015. Código de Processo Civil. *Diário Oficial da União*: Brasília, DF, 16 mar. 2015.
- BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). *Diário Oficial da União*: Brasília, DF, 14 ago. 2018.
- BRASIL. *Projeto de lei nº 2630, de 2020*. Institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet. Brasília, DF: Senado Federal, 2020. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2256735>. Acesso em 29 jun. 2024.
- BRASIL. Tribunal de Justiça do Estado de São Paulo. Apelação Cível nº XXXXX-38.2023.8.26.0100, da 34ª Câmara de Direito Privado do Tribunal de Justiça do Estado de São Paulo, São Paulo, SP, 25 de março de 2024. *Lex: jurisprudência do Tribunal de Justiça do Estado de São Paulo*. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tj-sp/2319355008/inteiro-teor-2319355017>. Acesso em 28 jun. 2024.
- BUENO, Thales M.; CANAAN, Renan G. The Brussels Effect in Brazil: Analysing the impact of the EU digital services act on the discussion surrounding the fake news bill. *Telecommunications Policy*, 48, p. 1-15, 2024. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0308596124000545#sec4>. Acesso em 29 jun. 2024.
- CATALAN, Marcos. Primeiras reflexões sobre o abuso de direito nas relações familiares. *IBDFAM: VI Congresso Brasileiro de Direito de Família*, nov. 2007. Disponível em:

- https://ibdfam.org.br/_img/congressos/anais/106.pdf. Acesso em 25 jun. 2024.
- CEYLAN, Gizem; ANDERSON, Ian A.; WOOD, Wendy. Sharing of misinformation is habitual, not just lazy or biased. *PNAS*, v. 120, n. 4, 2023. Disponível em: <https://www.pnas.org/doi/abs/10.1073/pnas.2216614120?af=R>. Acesso em 14 jun. 2024.
- CHEN, Yen-Shao; ZAMAN, Tauhid. Shaping opinions in social networks with shadow banning. *Plos One*, 19, 3, 2024. Disponível em: <https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0299977>. Acesso em 15 jun. 2024.
- CHENG, Shuyi. Automated content moderation. *Georgetown Law Technology Review*, 351, 2022.
- CHETTY, Raj *et al.* Social capital I: measurement and associations with economic mobility. *Nature*, 608, p. 108-121, 2022. Disponível em: <https://www.nature.com/articles/s41586-022-04996-4>. Acesso em 29 jun. 2024.
- CORDEIRO, Antônio. M. Do abuso do direito: estado das questões e perspectivas. *Revista da Ordem dos Advogados*, v. II, a. 65, set. 2005. Disponível em: <https://portal.oa.pt/publicacoes/revista-da-ordem-dos-advogados/ano-2005/ano-65-vol-ii-set-2005/artigos-doutrinais/antonio-menezes-cordeiro-do-abuso-do-direito-estado-das-questoes-e-perspectivas-star/#:~:text=%C3%89%20ileg%C3%ADtimo%20o%20exerc%C3%ADcio%20de,social%20ou%20econ%C3%B3mico%20desse%20direito>. Acesso em 26 jun. 2024.
- COTTER, Kelley. Playing the Visibility Game: How Digital Influencers and Algorithms Negotiate Influence on Instagram. *New Media and Society*, 21, 4, p. 895-913, 2019. Disponível em: <https://www.semanticscholar.org/paper/Playing-the-visibility-game%3A-How-digital-and-on-Cotter/3f94845cfec2ed04bfd0d0b1a41b994a56e5f6d9>. Acesso em 29 jun. 2024.
- COTTER, Kelley. “Shadowbanning is not a thing”: black box gaslighting and the power to independently know and credibly critique algorithms. *Information, Communication & Society*, v. 26, 2023. Disponível em: <https://www.tandfonline.com/doi/full/10.1080/1369118X.2021.1994624>. Acesso em 12 jun. 2024.
- DANTAS, Paulo R. F. *A proteção contra cláusulas abusivas no Código Civil*, São Paulo: Atlas, 2007.
- DIAS, Daniel; BELL, Luca; ZINGALES, Nicolo; GASPARE, Walter B.; CURZI, Yasmin. Plataformas no Marco Civil da Internet: a necessidade de uma responsabilidade progressiva baseada em riscos. *Civilistica.com*, a. 12, n. 3, 2023. Disponível em: <https://civilistica.emnuvens.com.br/redc/article/view/931/737>. Acesso em 14 jun. 2024.
- DONOVAN, Joan; BOYD, Danah. Stop the Presses? Moving from Strategic Silence to Strategic Amplification in a Networked Media Ecosystem. *American Behavioral Scientist*, 65, 2, p. 333-350, 2019. Disponível em: https://www.researchgate.net/publication/356909505_Stop_the_Presses_Moving_from_Strategic_Silence_to_Strategic_Amplification_in_a_Networked_Media_Ecosystem. Acesso em 29 jun. 2024.
- DOUEK, Evelyn. *Content Moderation as Systems Thinking*. Harvard Law Review. Cambridge:

- Harvard University Press. v. 136, n. 02, p. 526-607, dez. 2022.
- ENARSSON, Therese. Online Content Moderation in and Beyond the EU Digital Services Act – Exploring the Tension between Automated Speed and Human Contextuality. *SSRN*, abr. 2024. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4806704. Acesso em 15 jun. 2024.
- EUROPEAN UNION. Digital Services Act. *REGULATION (EU) 2022/2065 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC* (Digital Services Act). Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065>. Acesso em 13 jun. 2024.
- FERNANDES, Rodrigo. Seis polêmicas do TikTok em 2019. *Techtudo*, dez. 2019. Disponível em: <https://www.techtudo.com.br/noticias/2019/12/seis-polemicas-do-tiktok-em-2019.ghml>. Acesso em 17 jun. 2024.
- FLYVERBOM, Mikkel. *The Digital Prism: Transparency and managed visibilities in a datafied world*. New York: Cambridge University Press, 2019.
- FRAZÃO, Ana. *A nova Lei Geral de Proteção de Dados Pessoais: principais repercussões para a atividade empresarial*: parte I. 2018. Disponível em: https://www.professoraanafrazao.com.br/files/publicacoes/2018-08-30-A_nova_Lei_Geral_de_Protecao_de_Dados_Pessoais_Principais_repercussoes_para_a_atividade_empresarial_Parte_I.pdf. Acesso em 27 jun. 2024.
- GILLESPIE, Tarleton. Do Not Recommend? Reduction as a Form of Content Moderation. *Social Media + Society*. v. 8, i. 3, jul.-set. 2022. Disponível em: <https://journals.sagepub.com/doi/full/10.1177/20563051221117552>. Acesso em 13 jun. 2024.
- GILLESPIE, Tarleton. The Relevance of Algorithms. In: GILLESPIE, Tarleton; BOCZKOWSKI, Pablo; FOOT, Kirsten. *Media Technologies: Essays on Communication, Materiality, and Society*. Cambridge, MA: MIT Press. Disponível em: <https://www.semanticscholar.org/paper/The-Relevance-of-Algorithms-Gillespie-Boczowski/746fe3c376041dbd1a5a042584f47bff02c0d272>. Acesso em 14 jun. 2024.
- GOLDMAN, Eric. Content Moderation Remedies. *Michigan Technology Law Review*, v. 28, n.1, 2021. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3810580. Acesso em 14 jun. 2024.
- GOMES, Orlando. *Contratos de adesão: condições gerais dos contratos*, São Paulo: Revista dos Tribunais, 1972.
- JAIDKA, Kokil; MUKERJEE, Subhayan; LELKES, Yphtach. Silenced on social media: The gatekeeping functions of shadowbans in the American Twitterverse. *Journal of Communication*, abr. 2022. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4087843. Acesso em 13 jun. 2024.
- LAUTENSCHLÄGER, Milton F. A. C. Abuso de direito. *Enciclopédia Jurídica da PUC SP*. Tomo

- Direito Civil, ed. 1, dez. 2021. Disponível em: <https://enciclopediajuridica.pucsp.br/verbete/478/edicao-1/abuso-de-direito#:~:text=O%20C%C3%B3digo%20Civil%20de%202002,f%C3%A9%20ou%20pelos%20bons%20costumes%E2%80%9D>. Acesso em 25 jun. 2024.
- LEÃO, Luciana O. projeto de lei 2630/2020 – Lei das fake news – e o cenário da regulação em mercados digitais no Brasil diante do Digital Markets Act: um breve panorama. *IDP: Debates em Administração Pública*, v. 4, n. 3, 137, 2023. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/redap/article/view/7620>. Acesso em 29 jun. 2024.
- LEE, Edward. Moderating Content Moderation: A Framework for Nonpartisanship in Online Governance. *American University Law Review*. Washington: Washington College of Law. v. 70, n. 03, p. 913-1060, fev. 2021.
- LEERSSEN, Paddy. The Soap Box as a Black Box: Regulating Transparency in Social Media Recommender Systems. *European Journal of Law and Technology*, v. 11, n. 2, mar. 2020. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3544009. Acesso em 13 jun. 2024.
- LEERSSEN, Paddy. An end to shadow banning? Transparency rights in the Digital Services Act between content moderation and curation. *Computer Law & Security Review*, 48, p. 1-13, 2023. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0267364923000018>. Acesso em 13 jun. 2024.
- LEMOS, Ronaldo. O Marco Civil como símbolo do desejo por inovação no Brasil. In: LEITE, George S.; LEMOS, Ronaldo (Coords.). *Marco Civil da Internet*. São Paulo: Atlas, 2014.
- LONGONI KLEE, Antonia E. O conceito de estabelecimento empresarial virtual e a proteção do consumidor nos contratos eletrônicos: algumas reflexões. In: MARTINS, Guilherme Magalhães (Coord.). *Direito Privado e Internet*. São Paulo: Atlas, 2014.
- LUMIA, Giuseppe. *Teoria da relação jurídica: Lineamenti di teoria e ideologia del diritto*, 3. ed., Milano: Giuffrè, trad. Alcides Tomasetti Jr., 1981.
- MOREIRA, Arthur S.P.; DELGADO, Camila C. B.; SANTOS, Gabriel G. Repensando a tecnologia blockchain: por que nem tudo o que você leu até hoje era verdade? In: PARENTONI, Leonardo; MILAGRES, Marcelo de Oliveira; VAN DE GRAAF, Jeroen (Coords). MOREIRA, Arthur Salles de Paula; CHAGAS, Ciro Costa; SANTANA, Mariana Damiani (Orgs). *Direito, tecnologia e inovação – vol. III: Aplicações jurídicas de blockchain*. Expert: Belo Horizonte, 2021.
- MULLIGAN, Deirde, K.; BAMBERGER, Kenneth A. Allocating Responsibility in Content Moderation: A Functional Framework. *Berkeley Technology Law Journal*. Berkeley: University of California School of Law. v. 36, n. 03, p. 1091-1171, 2021.
- NICHOLAS, Gabriel. Sunsetting “Shadowbanning”. *Yale Law School Information Society Project Platform Governance Terminologies Essay Series*, jul. 2023. p. 4. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4522168. Acesso em 17 jun. 2024.

- OLIVA, Thiago D. Content Moderation Technologies: Applying Human Rights Standards to Protect Freedom of Expression. *Human Rights Law Review*, 20, p. 607–640, 2020. Disponível em: <https://academic.oup.com/hrlr/article/20/4/607/6023108>. Acesso em 14 jun. 2024.
- PASQUALE, Frank. *The black box society*. Harvard University Press, 2015.
- QUINTAIS, João P.; APPELMAN, Naomi; FATHAIGH, Ronan Ó. Using Terms and Conditions to apply Fundamental Rights to Content Moderation. *German Law Journal*, 24, pp. 881–911, 2023. p. 883. Disponível em: <https://www.cambridge.org/core/journals/german-law-journal/article/using-terms-and-conditions-to-apply-fundamental-rights-to-content-moderation/B30B9043D1C6F14AE9C3647A845E6E10>. Acesso em 17 jun. 2024).
- SCHNEIER, Bruce. *Secret & Lies: Digital Security in a Networked World*. Indianapolis: Wiley Publishing, 2000.
- SPAGNUOLO, Sergio. Twitter confirma shadow ban contra certos usuários. *Núcleo*, dez. 2022. Disponível em: <https://nucleo.jor.br/reportagem/2022-12-09-twitter-files-black-lists/>. Acesso em 17 jun. 2024.
- STRANGE, Susan. *States and markets: An introduction to International Political Economy*. London: Pinter Publishers, 1993. Disponível em: http://www.adelinotorres.info/desenvolvimento/SUSAN%20STRANGE_States%20and%20Markets_%20Susan%20Strange.pdf. Acesso em 14 jun. 2024.
- TEFFÉ, Chiara Spadaccini de; SOUZA, Carlos Affonso. Responsabilidade civil de provedores na rede: análise da aplicação do marco civil da internet pelo Superior Tribunal de Justiça. *Revista IBERC*, v.1, n. 1, nov.-fev./2019. Disponível em: <https://revistaiberc.responsabilidadecivil.org/iberc/article/view/6/5>. Acesso em 14 jun. 2024.
- THORSON, Kjerstin; WELLS, Chris. Curated Flows: A Framework for Mapping Media Exposure in the Digital Age. *Communication Theory*, v. 26, i. 3, ago. 2016. Disponível em: <https://doi.org/10.1111/comt.12087>. Acesso em 13 jun. 2024.
- TOMASEVICIUS FILHO, Eduardo. Marco Civil da Internet: uma lei sem conteúdo normativo. *Estudos Avançados*. São Paulo: Direito GV, v. 30, n. 86, p. 269-285, abr. 2016.
- TOMAZ, Tales. Brazilian Fake News Bill: Strong Content Moderation Accountability but Limited Hold on Platform Market Power. *Journal of the European Institute for Communication and Culture*, v. 30, i. 2, p. 253-267, 2023. Disponível em: <https://www.tandfonline.com/doi/full/10.1080/13183222.2023.2201801>. Acesso em 29 jun. 2024.

MODERAÇÃO AUTOMATIZADA EM REDES SOCIAIS E O NECESSÁRIO DIÁLOGO ENTRE A REGULAÇÃO DE PLATAFORMAS DIGITAIS E A REGULAÇÃO DA INTELIGÊNCIA ARTIFICIAL

Fernanda dos Santos Rodrigues Silva

Doutoranda em Direito pela Universidade Federal de Minas Gerais, na área de estudo Direito, Tecnologias e Interdisciplinaridade. Mestre em Direitos na Sociedade em Rede e graduada em Direito pela Universidade Federal de Santa Maria. Coordenadora de Pesquisa e Pesquisadora no Instituto de Referência em Internet e Sociedade (IRIS).

DOI: <https://doi.org/10.59224/dti7.ch9>

Resumo: O artigo investiga em que medida as regulações de inteligência artificial e de plataformas de redes sociais podem estabelecer um diálogo para enfrentar os desafios relacionados à moderação de conteúdo automatizada. Partindo do pressuposto de que o Marco Civil da Internet, embora importante, não responde a problemas atuais, o trabalho explora os desafios da IA na moderação, para compreender possíveis soluções. Nesse sentido, é investigada a complementaridade de medidas de mitigação que podem ser adotadas em uma regulação para inteligência artificial e uma para plataformas digitais para uma moderação automatizada mais segura e transparente.

Palavras-chave: inteligência artificial; moderação de conteúdo; regulação.

Abstract: The article investigates to what extent the regulations of artificial intelligence and social media platforms can establish a dialogue to address the challenges related to automated content moderation. Assuming that the Brazilian Internet Bill of Rights, although important, does not respond to current problems, the work explores the challenges of AI in moderation to understand possible solutions. In this sense, it explores the need for convergence between regulations for artificial intelligence and digital platforms for safer and more transparent moderation.

Keywords: artificial intelligence; content moderation; regulation.

SUMÁRIO: Introdução; 1. O Marco Civil da Internet e a evolução dos desafios da moderação de conteúdo em plataformas digitais; 2. Desafios da moderação de conteúdo

por IA e as ameaças a direitos fundamentais em plataformas digitais; 3. As interseções entre a regulação de plataformas e de inteligência artificial para uma moderação de conteúdo confiável e legítima; 3.1. Princípios e direitos para usuários de plataformas digitais e pessoas afetadas por sistemas algorítmicos; 3.2. Medidas de governança e transparência para agentes envolvidos com moderação automatizada de conteúdo; 4. Conclusão; Referências.

INTRODUÇÃO

O presente trabalho pretende responder à seguinte pergunta: em que medida as regulações de inteligência artificial e de plataformas de redes sociais podem estabelecer um diálogo para enfrentar os desafios relacionados à moderação de conteúdo automatizada? Para tanto, o artigo parte do pressuposto de que o Marco Civil da Internet (MCI) foi importante para responder aos desafios da sua época, em 2014, dentre os quais a moderação de conteúdo ainda não despertava tantas preocupações como atualmente. No entanto, ao longo da última década, os desafios mudaram, principalmente diante da ampliação do poder conferido a plataformas de redes sociais, que passaram a influenciar o debate político, econômico e social.

Com um número cada vez maior de usuários e de conteúdos compartilhados por minuto, esses intermediários tiveram de lançar mão de mecanismos automatizados mais complexos para realizar tarefas de moderação, ou seja, para definir o que pode e o que não pode circular em seu ambiente virtual. Enquanto uma atividade que impacta diretamente em direitos fundamentais, como a liberdade de expressão e de acesso à informação, torna-se relevante olhar com maior atenção para os possíveis desafios e problemas impostos por essa moderação automatizada.

Ao prever somente a responsabilidade de plataformas intermediárias em relação a conteúdo terceiros no caso de descumprimento de ordem judicial que obrigue à remoção específica, salvo no caso de violação de direitos autorais e conteúdo com nudez ou sexo sem consentimento, o MCI deixou em aberto a possibilidade de realização de uma moderação de conteúdo proativa. Ocorre que, diante da ausência de parâmetros e regras para essa tarefa, as plataformas de redes sociais operam com total autonomia em relação às suas políticas de comunidade e quais informações sobre moderação serão disponibilizadas para o público, que fica mais vulnerável diante da

opacidade desse tipo de atividade.

Em que pese não seja o objetivo deste trabalho discutir uma possível nova proposta de responsabilização de intermediários, a partir da análise dos desafios da moderação de conteúdo por IA em redes sociais, abordam-se os pontos de convergência entre a regulação de inteligência artificial e de plataformas de redes sociais, capazes de contribuir para uma moderação automatizada *accountable* e transparente. Em termos metodológicos, esta pesquisa é predominantemente indutiva, na medida em que parte de casos específicos relacionados à moderação de conteúdo automatizada, para traçar reflexões sobre a conexão entre uma regulação para IA e uma para plataformas digitais. Como método de procedimento, emprega-se a revisão de literatura exploratória, orientada a identificar medidas de mitigação para os riscos e desafios associados à moderação de conteúdo automatizada, por meio de pesquisa bibliográfica e documental. Os mecanismos de busca utilizados para a revisão bibliográfica foram o SciELO, Scholar Google, ResearchGate e Scopus.

1 O MARCO CIVIL DA INTERNET E A EVOLUÇÃO DOS DESAFIOS DA MODERAÇÃO DE CONTEÚDO EM PLATAFORMAS DIGITAIS

É possível afirmar que o Marco Civil da Internet representou um dos momentos mais significativos na história dos direitos digitais no Brasil. Apesar de seu processo de elaboração remontar formalmente ao ano de 2010, a sua construção derivou de anos de discussões em torno de como regular questões relacionadas à internet, ainda mais em um contexto em que os potenciais riscos e benefícios do ciberespaço pendiam de melhor compreensão e o acesso à rede mundial de computadores era mais restrito a uma parte da população do que atualmente.

Assim, enquanto a primeira legislação do seu gênero, o MCI destacou-se como referência para outros países. Dentre as suas principais previsões, está o regime de responsabilização de plataformas intermediárias, previsto em seu art. 19.¹ O dispositivo determina que a figura do provedor de serviços só poderá ser responsabilizada por conteúdo de terceiro no caso de descumprimento de decisão judicial que obrigue

1. BRASIL. *Lei nº 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 2 jul. 2024.

à sua remoção. Esse sistema, conhecido como *judicial notice and take down*, consolidou o caminho para as ações movidas por usuários contra plataformas, solicitando a remoção de conteúdos específicos.

Uma das suas exceções são conteúdos que contêm nudez ou cenas de sexo sem consentimento, situação em que as plataformas poderão ser responsabilizadas após receberem notificação extrajudicial por interessado qualificado e deixarem de agir (art. 21). Da mesma forma, conteúdo com violação de direitos autorais são excepcionados da responsabilização prevista no art. 19, cabendo à edição de lei específica tratar sobre o tema. No entanto, hoje o entendimento majoritário do Judiciário é de que também neste caso basta a notificação extrajudicial para que o conteúdo deva ser removido, sob pena de responsabilização.²

Em que pese não abordasse expressamente o conceito de moderação de conteúdo, assim como em nenhum outro momento do texto, o Marco Civil da Internet não vedou a possibilidade de que a própria plataforma realizasse essa atividade. Mesmo na ausência de uma cláusula como a chamada cláusula do “bom samaritano” na seção 230 do *Communications Decency Act*, nos Estados Unidos,³ verifica-se que a lei não estabeleceu sanções no caso de o próprio provedor proceder à remoção ou suspensão de postagens, conforme suas políticas de comunidade.

Tal previsão parecia responder bem aos anseios da época, ainda mais em um momento em que as plataformas digitais, principalmente de redes sociais, não eram tão grandes como atualmente. Segundo a pesquisa TIC Domicílios 2014,⁴ 50% dos domicílios brasileiros, considerando áreas urbana e rural, tinham acesso à internet através do computador e 47% através do celular. Em relação às atividades online, aqueles que acessavam a internet somente pelo computador, utilizavam-na mais para enviar e receber e-mails, encontrar informações sobre produtos e para fazer leituras de

2. VALENTE, Mariana. *Direito autoral e plataformas de internet: um assunto aberto*. InternetLab, 18 abr. 2019. Disponível em: <https://internetlab.org.br/pt/especial/direito-autoral-e-plataformas-de-internet-um-assunto-em-aberto/>. Acesso em: 17 jun. 2024.

3. ELECTRONIC FRONTIER FOUNDATION. Section 230. Disponível em: <https://www EFF.org/pt-br/issues/cda230>. Acesso em: 2 jul. 2024.

4. CETIC.BR. *Acesso à internet no Brasil: desafios para conectar toda a população*. Panorama Setorial da Internet, ano 8, n. 1, mar./2016. Disponível em: https://cetic.br/media/docs/publicacoes/6/Panorama_Setorial_11.pdf. Acesso em: 15 jun. 2024.

jornais, revistas ou notícias. As pessoas que acessavam pelo celular, por outro lado, utilizavam-no principalmente para enviar mensagens de texto, como pelo *Whatsapp*, e para acessar redes sociais, sendo 47% dos usuários.

Assim, ainda que o uso da internet já tivesse dado um salto em relação a anos anteriores, percebe-se que o desafio da própria conectividade permanecia como o maior problema a ser enfrentado – hoje, ele ainda é uma questão, com aproximadamente 36 milhões de brasileiros e brasileiras que seguem sem ter acesso à internet, mas soma-se à necessidade de ampliar a conectividade significativa, ou seja, melhorar a *qualidade* de acesso para aqueles que acessam a internet somente pelo celular e por um período de mês, por exemplo.⁵ O uso de redes sociais, por outro lado, já era visível, mas ainda inferior aos 80% de pessoas que, segundo a TIC Domicílios 2022, utilizavam a internet para acessar aplicativos como Facebook, Instagram ou TikTok.⁶

Segundo levantamento de 2023, essa preferência colocou o Brasil como o terceiro maior consumidor de redes sociais no mundo inteiro, ficando atrás apenas da Índia e Indonésia, mas sendo o maior da região da América Latina.⁷ Neste ponto, cumpre ressaltar que não se desconhece o fato de que o art. 19 ou o termo “plataformas digitais” não se referem somente a redes sociais.⁸

5. NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR (ed.). *Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros: TIC Domicílios 2022* [livro eletrônico]. São Paulo: Comitê Gestor da Internet no Brasil, 2023. Disponível em: https://www.cetic.br/media/docs/publicacoes/2/20230825143720/tic_domicilios_2022_livro_eletronico.pdf. Acesso em: 15 jun. 2024.
6. NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR (ed.). *Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros: TIC Domicílios 2022* [livro eletrônico]. São Paulo: Comitê Gestor da Internet no Brasil, 2023. Disponível em: https://www.cetic.br/media/docs/publicacoes/2/20230825143720/tic_domicilios_2022_livro_eletronico.pdf. Acesso em: 15 jun. 2024.
7. PACETE, Luiz Gustavo. *Brasil é o terceiro maior consumidor de redes sociais em todo o mundo*. *Forbes*, Forbes Tech, 9 mar. 2023. Disponível em: <https://forbes.com.br/forbes-tech/2023/03/brasil-e-o-terceiro-pais-que-mais-consome-redes-sociais-em-todo-o-mundo/>. Acesso em: 15 jun. 2024.
8. De fato plataformas digitais podem ser consideradas “como sistemas tecnológicos em que se desenvolvem atividades sobre uma base tecnológica, comandados por proprietários (uma empresa, como no caso do Google, ou cooperativas, como a plataforma de comércio europeia Fairmondo), mas dos quais participam outros agentes (produtores, intermediários, usuários), cujos controle e

Entretanto, apesar de o conceito abordar uma ampla gama de possibilidades, para os fins deste texto, importam especificamente os desafios de moderação de conteúdo no espaço de redes sociais, considerando o seu especial impacto e poder atualmente. Deste modo, as expressões “plataforma digital”, “intermediários” e “provedores de serviço”, neste contexto, serão utilizados como sinônimos de redes sociais.

Nessa mesma direção, destaca-se que o que se entende por moderação de conteúdo traduz, na verdade, um “conjunto de ações realizadas pelos provedores de plataformas digitais, no sentido de exercer a intervenção ou curadoria em relação aos conteúdos” disponibilizados por terceiros em seu espaço digital⁹. Assim, considera-se tanto a sua função de sanitização do ambiente virtual, com a adequação dos usuários às políticas da plataforma e remoção ou suspensão de conteúdo nocivo e contas violadoras, como a sua função enquanto produto, ou seja, enquanto um serviço que a plataforma oferece aos usuários.¹⁰

Com efeito, a massificação do uso de redes sociais representou um significativo aumento do poder conferido a essas empresas, na medida em que o escopo da moderação de conteúdo atinge diretamente direitos fundamentais, como os direitos à liberdade de expressão e de acesso à informação. Enquanto detentoras da competência de definir o que pode ou não circular nos seus espaços, o que será visto por mais pessoas e os conteúdos que terão seu alcance reduzido, as plataformas de redes

gestão jogam papel organizador chave e nos quais operam lógicas econômicas, práticas culturais e normas diversa (regulatórias e internas), a partir das quais os ST promovem uma mediação ativa nas atividades onde estão inseridas”. VALENTE, Jonas. *Tecnologia, informação e poder: das plataformas online aos monopólios digitais*. Tese (Doutorado em Sociologia) – Universidade de Brasília, Brasília, 2019, 399p, p. 169.

9. SILVA, Fernanda dos Santos Rodrigues; GERTRUDES, Júlia Maria Caldeira; SILVA, Rafaela Ferreira Gonçalves da. *Regulação de plataformas e devido processo na moderação de conteúdo: perspectivas em 5 continentes*. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2024, p. 10. Disponível em: <https://irisbh.com.br/publicacoes/devido-processo-na-moderacao-de-conteudo-em-5-continentes/>. Acesso em: 15 jun. 2024.
10. SILVA, Fernanda dos Santos Rodrigues; GERTRUDES, Júlia Maria Caldeira; SILVA, Rafaela Ferreira Gonçalves da. *Regulação de plataformas e devido processo na moderação de conteúdo: perspectivas em 5 continentes*. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2024, p. 10. Disponível em: <https://irisbh.com.br/publicacoes/devido-processo-na-moderacao-de-conteudo-em-5-continentes/>. Acesso em: 15 jun. 2024.

sociais operam como verdadeiros controladores da circulação de discursos.

Em um cenário em que 51% dos brasileiros e brasileiras consomem notícias através das redes sociais¹¹ e somente 37% dos usuários que acessam internet apenas pelo celular checam se as informações que encontram online são verdadeiras,¹² a moderação realizada pelas plataformas torna-se efetivamente capaz de influenciar o debate político, social e econômico para uma grande quantidade de pessoas e, por consequência, influenciar esse mesmo debate para além das fronteiras do seu espaço digital. Ao mesmo tempo, como já mencionado, não há como deixar de lado a importância da moderação de conteúdo para a manutenção de um espaço seguro e saudável para que os usuários possam interagir livremente.

Segundo o relatório de transparência mais recente da Meta, referente ao primeiro trimestre de 2024 e em âmbito mundial, foram moderados 8,6 milhões de conteúdos contendo discurso de ódio¹³ e 12,3 milhões contendo violência e incitação¹⁴ no Instagram. Por outro lado, 2,2 milhões e 1,6 milhões das pessoas que tiveram seu conteúdo moderado, respectivamente, por cada uma dessas razões, recorreram da decisão da plataforma, sendo restaurados 142 mil e 287 mil conteúdos após as contestações. Estes números demonstram que, apesar de importante, nem sempre a atividade de moderação atua corretamente em todos os casos. Mesmo que represente uma porcentagem pequena em relação ao total de casos em que plataforma atua, é necessário atenção para que esse fato não acabe por legitimar um suposto grau de eficiência dos

11. NEWMAN, Nic et al. *Digital News Report 2024*. Oxford: Reuters Institute, University of Oxford, 2024. Disponível em: <https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2024-06/DNR%202024%20Final%20lo-res-compressed.pdf>. Acesso em: 17 jun. 2024.

12. NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR (ed.). *Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros: TIC Domicílios 2022* [livro eletrônico]. São Paulo: Comitê Gestor da Internet no Brasil, 2023. Disponível em: https://www.cetic.br/media/docs/publicacoes/2/20230825143720/tic_domicilios_2022_livro_eletronico.pdf. Acesso em: 15 jun. 2024.

13. META. *Community Standards Enforcement Report: hate speech*. Disponível em: <https://transparency.meta.com/reports/community-standards-enforcement/hate-speech/instagram/>. Acesso em: 17 jun. 2024.

14. META. *Community Standards Enforcement Report: violence and incitement*. Disponível em: <https://transparency.meta.com/reports/community-standards-enforcement/violence-incitement/instagram/>. Acesso em: 17 jun. 2024.

mecanismos de moderação, na medida em que esse número “baixo” ainda significa centenas de milhares de decisões equivocadas.¹⁵

Além disso, acusações de enviesamento na forma com que plataformas de redes sociais atuam geram uma sensação de desconfiança em como a moderação é feita. Estudos que apontam a necessidade de um compromisso maior por parte de intermediários com uma moderação de conteúdo imparcial, especialmente em casos envolvendo políticos e campanhas, por exemplo, são um termômetro para a necessidade de balizas que gerem uma *accountability* em torno dessa atividade.¹⁶

Essa realidade, portanto, demonstra uma importante mudança no cenário que havia quando o Marco Civil da Internet foi aprovado, em 2014. Salvo no caso de nudez e violação de direitos autorais, em que a responsabilidade da plataforma incide logo após mera notificação extrajudicial, gerando um estímulo para que elas removam esse tipo de conteúdo de forma mais célere, a regra geral do art. 19 permite que estabeleçam seu próprio ritmo e gerenciamento da atividade de moderação. No entanto, em uma realidade com crescente número de compartilhamentos de conteúdo em redes sociais, uma moderação morosa ou equivocada pode ter um impacto muito mais substantivo do que há uma década.

A utilização de ferramentas de moderação de conteúdo automatizadas, por sua vez, necessárias em razão desse número exacerbado de conteúdo postado, adiciona uma camada de opacidade ao não se ter nitidez sobre quais critérios são utilizados para rotular determinado conteúdo como nocivo e outro não. Neste ponto, o próximo capítulo cuidará de abordar especificamente os desafios apresentados por estas ferramentas, a fim de compreender posteriormente em que medida uma convergência entre as regulações para IA e plataformas de redes sociais podem contribuir enfrentá-los.

15. SILVA, Fernanda dos Santos Rodrigues; GERTRUDES, Júlia Maria Caldeira. *Governança da moderação de conteúdo online: percepções sobre o papel dos atores e regimes*. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2023, p. 29. Disponível em: <https://bit.ly/3WHMUlg>. Acesso em: 17 jun. 2024.

16. LEE, Edward. Moderating Content Moderation: A Framework for Nonpartisanship in Online Governance. *American University Law Review*, v. 70, n. 03, p. 913-1060, fev. 2021.

2 DESAFIOS DA MODERAÇÃO DE CONTEÚDO POR IA E AS AMEAÇAS A DIREITOS FUNDAMENTAIS EM PLATAFORMAS DIGITAIS

Segundo pesquisa realizada pela empresa de serviço de computação em nuvem, Domo, em 2022, a cada minuto, foram compartilhadas 66 mil fotos no Instagram; 347,2 mil tweets no antigo Twitter – agora X; e 1,7 milhões de “pedaços de conteúdo” no Facebook.¹⁷ Diante da impossibilidade de se moderar essa quantidade de conteúdo somente por moderação humana, a moderação automatizada, feita com o auxílio de sistemas de inteligência artificial, é uma realidade para grandes empresas de rede social. Com a competência para poder estabelecer os melhores mecanismos para realizar essa atividade, as plataformas puderam desenvolver não só regras, como “tecnologias para bloquear, filtrar e monitorar a fala do usuário de forma voluntária”¹⁸.

De modo geral, dentre a variedade de técnicas disponíveis para moderação de conteúdo automatizada, existem duas formas principais através das quais uma máquina pode identificar e rotular conteúdo: por *matching* (correspondência), que seria a comparação entre a nova informação e o que já existe em uma base de dados prévia, e por *prediction* (predição), quando o aprendizado prévio da máquina é utilizado para identificar e analisar as características da nova informação.¹⁹ Na primeira, destaca-se o método de *hashing*, em que conteúdos como imagem e vídeo são transformados em uma única cadeia de dados (*hash*) para serem rotulados, permitindo ao sistema comparar rapidamente o valor atribuído ao *hash* com o valor na base dados, que possui *hashes* de conteúdos indesejados, como conteúdos nocivos.

No caso do *hashing* criptográfico, um *hash* de alta sensibilidade a alterações é utilizado para identificar correspondências, como para fins de autenticação de informações. Entretanto, ele não funciona adequadamente para moderação de conteúdo, uma vez que pode ser facilmente burlado através de pequenas alterações, como

17. DOMO. *Data never sleeps 10.0*. Disponível em: <https://web-assets.domo.com/miyagi/images/product/product-feature-22-data-never-sleeps-10.png>. Acesso em: 17 jun. 2024.

18. BLOCH-WEBER. Hannah. *Automation in Moderation*. Cornell International Law Journal, v. 53, 2020, pp. 41-96, p. 48. Disponível em: <https://community.lawschool.cornell.edu/wp-content/uploads/2021/03/Bloch-Wehba-final.pdf>. Acesso em: 17 jun. 2024.

19. SHENG, Chuyi. *Automated Content Moderation*. Georgetown Law Technology Review, v. 06, n. 01, p. 351-363, Jun. 2022, p. 355.

marcas d'água. O *hashing* perceptivo, por outro lado, cujo foco para determinar o limiar de diferença permitido entre dois *hashes* está nas características específicas do conteúdo, buscando identificar se a nova informação é similar o suficiente ao que já existe na base de dados,²⁰ constitui hoje o método considerado mais adequado para moderação de conteúdo, já que compreende melhor a relação entre duas imagens e não é afetado por pequenas mudanças no conteúdo.²¹ Além disso, trata-se de um método mais transparente, ao passo que é possível auditar os conteúdos de qualquer base de dados de *hash*, ao contrário de ferramentas mais opacas de IA para moderação de conteúdo, bem como por possuir uma natureza mais direcionada, ao contrário de IAs de generalização imprevisível.²²

Dentre as suas limitações, porém, são apontadas a possibilidade de sua utilização por governos totalitários ou com abuso de poder por parte de provedores de serviço, além da probabilidade de erro sobre conteúdos ilegais ou inapropriados que são mais difíceis de definir, como discurso de ódio, por exemplo.²³ Em razão disso, é importante que diferentes métodos sejam combinados, inclusive com o uso de moderação humana, a fim de enfrentar os diferentes desafios da moderação de conteúdo.

Em relação aos mecanismos de predição, por outro lado, destaca-se o processamento de linguagem natural, com o auxílio de redes neurais, para a moderação de conteúdos em texto. Através dela, há uma análise e classificação das diferentes características dos textos, com auxílio de categorização por humanos, a fim de treinar o sistema sobre essas categorias. Com a conversão de palavras, frases e estruturas em valores numéricos, as características são processadas e regras internas são criadas para atribuir pesos diferentes a cada uma e, posteriormente, novos exemplos de textos são analisados a partir do *framework* construído pelo sistema.²⁴ Por outro lado, a predição também é feita para moderação de conteúdo de imagem e vídeo, quando o sistema é capaz de analisar formas, texturas, cores, arranjo espacial e outros para

20. SHENG, Chuyi. *Automated Content Moderation*. Georgetown Law Technology Review, v. 06, n. 01, p. 351-363, Jun. 2022, p. 356-357.

21. *Ibid.*

22. FARID, Hany. *An Overview of Perceptual Hashing*. Journal of Online Trust and Safety, v. 1, n. 1, 2021. Disponível em: <https://tsjournal.org/index.php/jots/article/view/24>. Acesso em: 2 jul. 2024.

23. *Ibid.*

24. SHENG, Chuyi. *Op. cit.*, p. 359.

poder fazer a identificação.²⁵

Todas essas técnicas possibilitam que as plataformas ajam de maneira mais rápida e eficiente em seus ambientes e com benefícios reconhecidos, como não depender somente de moderação humana, escalabilidade, custos baixos e celeridade.²⁶ No entanto, quando se está falando de milhões de conteúdos moderados diariamente, mesmo a menor taxa de erros pode significar um alto número de pessoas impactadas equivocadamente por esses sistemas. Mais do que isso, a ausência de compreensão nítida sobre como essas ferramentas funcionam soma-se à ausência de regras na forma com que a moderação de conteúdo deve ser feita, deixando o usuário duplamente vulnerável.

Nesse sentido, diferentes desafios são listados pela literatura especializada em torno do uso de ferramentas de IA para fins de moderação de conteúdo em redes sociais. Um deles, e talvez o mais conhecido, sejam os riscos de erro que essas ferramentas têm na *(I) análise de contexto*. Apesar de também poder ocorrer sobre conteúdos imagéticos, como referido anteriormente, o erro na análise de contexto é muito comum na moderação de texto. Como mencionado anteriormente, essa moderação opera principalmente a partir das regras criadas para compreensão dos caracteres numéricos que representam palavras, frases e estruturas. Entretanto, é comum uma dificuldade na sintonia fina em situações em que o contexto dessas categorias pode ter um peso maior e uma deficiência na sua identificação acabar gerando uma moderação incorreta.

Um exemplo notório dessa situação são casos em que pessoas de grupos minoritários possuem seu conteúdo removido ou suspenso quando denunciam casos de discurso de ódio ou ressignificam palavras que em outra situação poderiam adquirir sentidos pejorativos. No caso de pessoas negras, por exemplo, há até mesmo uma expressão para quando, no Estados Unidos, seu conteúdo denunciando racismo é derrubado em plataformas digitais de Marck Zuckerberg, como Facebook e Instagram, que é *getting zucked*, ou, em tradução livre, algo como “*ser zuckeado*”.²⁷

25. *Ibid.*

26. *Ibid.*

27. GRAY, Kishonna L. STEIN, Krysten. “We ‘said her name’ and got zucked”: Black Women calling-out the carceral logics of digital platforms. *Gender & Society*, v. 35, n. 4, ago./2021, pp. 538-545.

Pessoas transgêneros são outro grupo vulnerabilizado, também tendo a maior parte de suas postagens derrubada quando publicam algum conteúdo envolvendo sua identidade já marginalizada²⁸ ou ressignificam termos que em outros casos poderiam ser ofensivos.²⁹

Atualmente, as políticas sobre discurso de ódio da Meta reconhecem expressamente a possibilidade de pessoas compartilharem conteúdo com calúnias ou discurso de ódio com a finalidade de “condenar essas práticas ou aumentar a conscientização”, assim como para “usar de forma autorreferencial ou empoderadora”.³⁰ No entanto, destacam ser necessário que a intenção da publicação seja apresentada de maneira clara, a fim de evitar sua remoção. Ocorre que o erro na identificação de contexto sobre publicações em que grupos minoritários expressam questões relacionadas à sua identidade, seja ela racial, de gênero ou outra, também podem ser classificados como (II) *vieses discriminatórios*.

Um caso significativamente emblemático desse tipo de viés foi a denúncia do artista Gabriel Jardim, que foi contratado para fazer uma ilustração em homenagem ao piloto de Fórmula 1, Lewis Hamilton. Na imagem, Gabriel retratou Hamilton ao fundo de um cenário de favela, em que um menino negro também aparece, descendo uma ladeira com carrinho de rolimã, como se fosse inspirado pelo piloto.³¹ Todavia,

Disponível em: <https://journals.sagepub.com/doi/pdf/10.1177/08912432211029393>. Acesso em: 16 jun. 2024.

28. HAIMSON, Oliver et al. *Disproportionate Removals and Differing Content Moderation Experiences for Conservative, Transgender, and Black Social Media Users: Marginalization and Moderation Gray Areas*. Proceedings of the ACM on Human-Computer Interaction, v. 5, n. 466pp 1–35, out./ 2021. Disponível em: <https://dl.acm.org/doi/10.1145/3479610>. Acesso em: 16 jun. 2024.

29. GOMES, Alessandra. ANTONIALLI, Dennys. OLIVA, Thiago. *Drag queens e Inteligência Artificial: computadores devem decidir o que é ‘tóxico’ na internet?* InternetLab, 28 jun. 2019. Disponível em: <https://internetlab.org.br/pt/noticias/drag-queens-e-inteligencia-artificial-computadores-devem-decidir-o-que-e-toxico-na-internet/>. Acesso em: 16 jun. 2024.

30. META. *Facebook Community Standards: hate speech*. Disponível em: https://transparency.meta.com/pt-br/policies/community-standards/hate-speech/?source=https%3A%2F%2Fwww.facebook.com%2Fcommunitystandards%2Fhate_speech. Acesso em: 16 jun. 2024.

31. LIRA, Isadora. *(In)visibilidades na rede: discurso de ódio e censura das plataformas*. Le Monde Diplomatique Brasil. 25 mai. 2022. Disponível em: <https://diplomatie.org.br/invisibilidades-na-rede-discurso-de-odio-e-censura-das-plataformas/>. Acesso em: 2 jul. 2024.

de maneira equivocada, a moderação de conteúdo do Instagram, onde a foto foi posta pelos contratantes de Gabriel, impediu o impulsionamento da ilustração, sob a justificativa de que ela promoveria “*venda de munição, armas de fogo, armas de paintball, armas de chumbinho*”, dentre outros. Em nenhum momento, porém, é possível identificar tais alusões, abrindo margem para a compreensão de que algo na imagem indicou algum tipo de associação nesse gênero.

Imagem 1 – Postagem com a ilustração encomendada no perfil de Gabriel Jardim no Instagram.



Fonte: reprodução / instagram @ogabrieljardim.³²

Imagem 2 – Postagem com resposta da plataforma ao pedido de impulsionamento, no perfil de Gabriel Jardim no Instagram.

32. Disponível em: https://www.instagram.com/ogabrieljardim/p/B5HJrglJHq/?img_index=1. Acesso em: 2 jul. 2024.



Fonte: reprodução / instagram @ogabrieljardim.³³

Essa denúncia reforça a preocupação em torno da reprodução de estereótipos nocivos sobre comunidades marginalizadas, como é o caso de comunidades periféricas e pretas no Brasil. Em 2015, um estudo conduzido pelo Instituto Data Popular já apontava que 69% dos entrevistados afirmaram ter medo ao passar próximo de uma favela, enquanto 51% referiram associar drogas e violências como as primeiras coisas que passam à cabeça quando ouvem falar desse lugar.³⁴ A utilização de uma ferramenta de moderação de conteúdo que pode potencializar esse tipo de preconceito, portanto, é significativamente perigoso, representando a revalidação de discursos que servem para a constante criminalização desse público.³⁵

33. Disponível em: https://www.instagram.com/ogabrieljardim/p/B5HJrgljHq/?img_index=1. Acesso em: 2 jul. 2024.

34. GANDRA, Alana. *Moradores do asfalto têm visão preconceituosa de favelas, mostra pesquisa*. Agência Brasil, 16 fev. 2015. Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2015-02/moradores-do-asfalto-tem-visao-preconceituosa-em-relacao-favelas>. Acesso em: 2 jul. 2024.

35. É possível afirmar que, em casos como esse, a máquina “promove decisões automatizadas a partir desses inputs amostrais e enviesados, fomenta processos e tomadas de decisões humanas e

Outra limitação da moderação de conteúdo por IA está nos *(III) erros na detecção de línguas ou dialetos específicos*. Frequentemente, ferramentas de moderação algorítmicas funcionam melhor para alguns idiomas do que para outros, sendo que o mais comum é que sejam treinadas em bases de dados em inglês. Isso aponta para questões éticas e até mesmo legais sobre a ideia de justiça quando se trata de padrões iguais para moderação de conteúdo aplicável em diferentes línguas,³⁶ uma vez que cada idioma possui suas particularidades, assim como cada país. Ao identificar expressões características do dialeto afro-americano como texto com alto nível de toxicidade, por exemplo, apontando para uma moderação mais rigorosa sobre esse tipo de conteúdo, nota-se um exemplo não somente de viés discriminatório, como da própria ineficiência no reconhecimento de dialetos específicos.³⁷

A *(IV) falta de transparência e explicabilidade* sobre como operam os sistemas de moderação de plataformas de redes sociais, porém, dificulta até mesmo que a fonte dos problemas possa ser adequadamente encontrada. Este ponto, em específico, merece atenção detalhada, na medida em que se subdivide em dois principais aspectos: o primeiro é que pouco se sabe sobre quais ferramentas de IA são responsáveis pela moderação nessas plataformas, quais foram suas bases de treinamento e quais critérios orientam sua atuação. O segundo é que, apesar de normalmente prever quais conteúdos são proibidos em seu espaço, as políticas de comunidade trazem pouca ou nenhuma informação sobre como ocorre o procedimento de moderação de conteúdo, como prazos para avaliação de contestação, e não explicitam de forma fundamentada quais termos foram violados em casos concretos.

Essa opacidade é vista até mesmo dentro de uma lógica intencional da plataforma

institucionais que promovem a discriminação racial, isto é, o tratamento diferenciado a membros de grupos racialmente identificados”. KREMER, Bianca. *Racismo algorítmico*. Rio de Janeiro: CE-SeC, 2023, p. 30.

36. PREM, Erich. KRENN, Brigitte. *On Algorithmic Content Moderation*. In: WERTHNER, Hannes. *Introduction to Digital Humanism: a textbook*. Cham: Springer, 2024, p. 481. Disponível em: https://link.springer.com/chapter/10.1007/978-3-031-45304-5_30. Acesso em: 16 jun. 2024.

37. SAP, Maarten. et al. *The Risk of Racial Bias in Hate Speech Detection*. Proceedings of the 57th Annual Meeting of the Association for Computational Linguistics, pp. 1668–1678, Florence, Italy, July 28 - August 2, 2019. Association for Computational Linguistics. Disponível em: <https://maartensap.com/pdfs/sap2019risk.pdf>. Acesso em: 2 jul. 2024.

para alguns autores, como Sarah Roberts.³⁸

Nesse sentido, para a autora, a plataforma se beneficiaria da falta de transparência sobre como opera sua moderação de conteúdo, em especial considerando o fato de que a opacidade teria o condão de trazer objetividade sobre seu *modus operandi* frente à imaginação pública. Em outras palavras, a opacidade contribuiria para que a atuação das plataformas passasse a ser vista como despida de qualquer subjetividade, o que elimina margens para questionamentos em torno das políticas e valores que orientam sua tomada de decisão.³⁹

Quando se observa a moderação de conteúdo para além remoção ou suspensão de contas e postagens, ou seja, para a forma com que se dá a curadoria e recomendação de conteúdos, em tese, com base nas preferências do usuário, os riscos associados à opacidade ganham ainda maior relevo. Isto, pois nem sempre usuários têm consciência de que há uma interferência da plataforma na ordem com que os conteúdos

38. Sarah Roberts afirma que “Obfuscation and secrecy work together to form an operating logic of opacity around social media moderation. It is a logic that has left users typically giving little thought to the mechanisms that may or may not be in place to govern what appears, and what is removed, on a social media site. The lack of clarity around policies, procedures and the values that inform them can lead users to have wildly different interpretations of the user experience on the same site. (...) Moreover, the lack of official information from social media firms pertaining to the decisions and operations surrounding what material is deemed acceptable and not further renders the machinery of content moderation opaque”. Tradução nossa: Ofuscação e segredo trabalham juntos para formar uma lógica operativa de opacidade em torno da moderação das redes sociais. É uma lógica que geralmente faz com que os usuários não pensem muito nos mecanismos que podem ou não estar em vigor para governar o que aparece e o que é removido em um site de mídia social. A falta de clareza em torno das políticas, procedimentos e os valores que os informam pode levar os usuários a terem interpretações amplamente diferentes da experiência do usuário no mesmo site. (...) Além disso, a falta de informações oficiais das empresas de redes sociais sobre as decisões e operações em torno do que é considerado material aceitável e o que não é torna ainda mais opaco o maquinário da moderação de conteúdo. In: ROBERTS, Sarah T. *Digital detritus: 'Error' and the logic of opacity in social media content moderation*. First Monday, v. 23 n. 3 mar. 2018. Disponível em: <https://firstmonday.org/ojs/index.php/fm/article/view/8283/6649>. Acesso em: 16 jun. 2024.

39. ROBERTS, Sarah T. *Digital detritus: 'Error' and the logic of opacity in social media content moderation*. First Monday, v. 23 n. 3 mar. 2018. Disponível em: <https://firstmonday.org/ojs/index.php/fm/article/view/8283/6649>. Acesso em: 16 jun. 2024.

são apresentados para eles na tela inicial da rede social e nos anúncios que são apresentados para as suas contas – assim como naqueles conteúdos que *não serão* recomendados ou impulsionados para eles de forma alguma.

O impacto dessa espécie de moderação é considerado tão significativo que há autores que defendem a ideia de uma governamentalidade algorítmica, que pode ser traduzida como “*um certo tipo de racionalidade (a)normativa ou (a)política que repousa sobre a coleta, a agregação e a análise automatizada de dados em quantidade massiva, de modo a modelizar, antecipar e afetar, por antecipação, os comportamentos possíveis*”⁴⁰. Nesse contexto, uma vez que a atenção dos indivíduos passa a ser conduzida para determinadas coisas, o foco é em ações que ajam sobre o ambiente, de modo a enviar sinais que provoquem ou estimulem certas respostas.⁴¹

Em razão disso, a curadoria e recomendação de conteúdos expõem um desafio diretamente relacionado à capacidade de plataformas digitais resultarem em uma (V) *modulação de comportamentos dos usuários*, o que geralmente pode acontecer sem o consentimento destes. Uma vez que há escassa informação sobre o método de funcionamento dos algoritmos que ordenam as chamadas “linhas do tempo” dos perfis pessoais, a disposição de postagens e informações pode ser lida com aparente neutralidade, invisibilizando a influência que as redes sociais operam sobre a subjetividade dos indivíduos.

Para além da esfera individual, essa modulação se torna ainda mais crítica por ser capaz de gerar (VI) *impactos no debate público*. As lógicas emergentes das plataformas, amplamente orientadas pela maximização do lucro, podem levar a uma apropriação do discurso como ferramenta de impulsionamento do engajamento de usuários através da distribuição algorítmica de conteúdo.⁴² Desse modo, a determinação

40. ROUVROY, Antoinette; BERNIS, Thomas. *Governamentalidade algorítmica e perspectivas de emancipação: o dispar como condição de individuação pela relação?* In: BRUNO, Fernanda et al. *Tecnopolíticas da vigilância: perspectivas da margem*. São Paulo: Boitempo, 2018, p. 115-116.

41. ALVES, Marco Antônio Sousa. *A resistência à governamentalidade algorítmica: condutas e contracondutas na era da informação*. In: MATOS, Andityas Soares de Moura Costa (org.). *Ensaio de desobediência epistemocrítica: dimensões antagonistas na era das sujeições bio-político-ciberneticas*. Belo Horizonte: Initia Via, 2019.

42. RIMER, K; PETER, S. *Algorithmic audiencing: Why we need to rethink free speech on social media*. Research Paper, Australia, v. 36, 4, p. 409-426, dez, 2021. Disponível em:

algorítmica das audiências “*apresenta uma interferência na liberdade de expressão porque distorce o discurso, amplificando ou suprimindo o alcance das mensagens com base em lógicas externas a esse discurso*”⁴³. Assim, o debate público pode ser diretamente influenciado pela conformação das discussões através da moderação feita por sistemas de inteligência artificial, o que pode levar a efeitos como as chamadas “câmaras de eco” ou até mesmo polarizações do debate político.⁴⁴

3 AS INTERSECÇÕES ENTRE A REGULAÇÃO DE PLATAFORMAS E DE INTELIGÊNCIA ARTIFICIAL PARA UMA MODERAÇÃO DE CONTEÚDO CONFIÁVEL E LEGÍTIMA

Os desafios da moderação de conteúdo automatizada esboçados no capítulo anterior demonstram que a ausência de definições e regras mais claras para essa atividade no Marco Civil da Internet já não encontra mais suporte. A complexidade em torno dessa tarefa aponta, na verdade, para a insuficiência de somente um único diploma legal capaz de fazer frente a todas as suas especificidades. Isto, porque uma primeira questão a ser observada é justamente o fato de que a moderação automatizada de conteúdo em redes sociais reúne, pelo menos, duas discussões: uma delas diz respeito à governança e *accountability* de sistemas de inteligência artificial utilizados para esta finalidade; e a outra, sobre a governança e *accountability* de plataformas de redes sociais.

Em outras palavras, isso significa que medidas de mitigação para os desafios

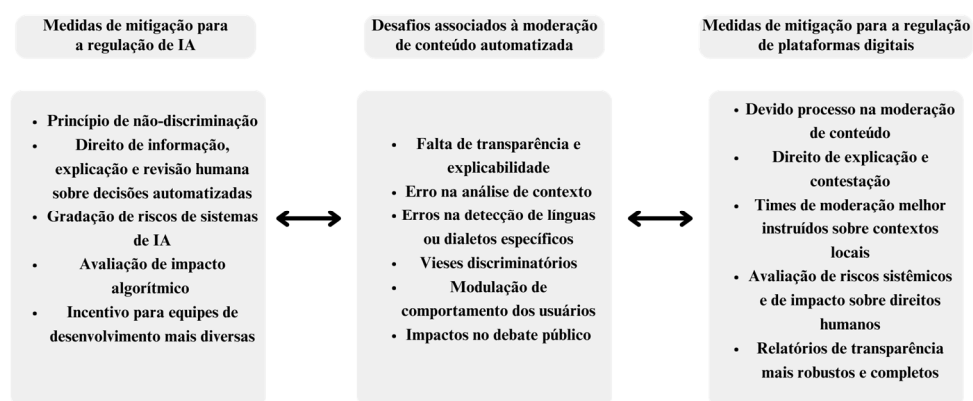
<https://ses.library.usyd.edu.au/bitstream/handle/2123/25053/publisher%20author%20accepted%20manuscript.pdf?sequence=1&isAllowed=y>. Acesso em: 17 jun. 2024.

43. “Algorithmic audiencing presents an interference with free speech because it distorts speech, amplifying or suppressing the reach of messages based on logics external to that speech”. In: RIMER, K; PETER, S. *Algorithmic audiencing: Why we need to rethink free speech on social media*. Research Paper, Australia, v. 36, 4, p. 409-426, dez, 2021. Disponível em: <https://ses.library.usyd.edu.au/bitstream/handle/2123/25053/publisher%20author%20accepted%20manuscript.pdf?sequence=1&isAllowed=y>. Acesso em: 17 jun. 2024.

44. FERREIRA, Sérgio Rodrigo da Silva. *Repensar a esfera pública política a partir das Câmaras de Eco: conceitos e questões metodológicas*. Liinc em Revista, Rio de Janeiro, v. 18, n. 2, e6067, nov.2022. Disponível em: <https://revista.ibict.br/liinc/article/view/6067/5694>. Acesso em: 17 jun. 2024.

mencionados anteriormente podem ser abordadas pelos dois caminhos. A imagem abaixo traz o esforço de tentar sumarizar as principais medidas que podem ser previstas nos dois tipos de regulações:

Imagem 3 - Panorama de principais medidas de mitigação para os riscos associados à moderação de conteúdo automatizada em regulações de inteligência artificial e de plataformas digitais.



Fonte: elaboração própria com base em literatura analisada.

Apesar de não ser um quadro exaustivo sobre as possíveis medidas de mitigação, a lista acima traz exemplos importantes mencionados na literatura especializada e que podem ser divididos em dois eixos principais: a) princípios e direitos para usuários de plataformas digitais e pessoas afetadas por sistemas algorítmicos; e b) medidas de governança e transparência para agentes envolvidos com moderação automatizada de conteúdo.

3.1 Princípios e direitos para usuários de plataformas digitais e pessoas afetadas por sistemas algorítmicos

A literatura sobre formas de lidar com desafios relacionados à moderação de conteúdo automatizada e sistemas de inteligência artificial em geral têm destacado o papel de assegurar direitos às possíveis pessoas afetadas. No campo da regulação de

plataformas, destacam-se o direito à explicação e contestação de decisões automatizadas.

No caso de medidas de contestação, autores defendem sua aplicação tanto para fins de denúncia de conteúdo nocivo quanto para revisão de decisões de remoção.⁴⁵ Essa seria uma forma de reparação individual, em prol da proteção do direito à liberdade de expressão, e se basearia na justificativa de que “*à medida que as plataformas aumentam de tamanho e poder, suas decisões de sancionar usuários tornam-se compatíveis às decisões que um Estado impõe sobre seus cidadãos, e suas políticas se assemelham a leis, tornando-as os ‘novos governantes’*” (tradução nossa).⁴⁶ Assim, se diante de um Estado é possível contestar ilegalidades, da mesma forma deve poder ser feito perante as plataformas.

O direito à explicação, por outro lado, é visto como relevante em especial para a recomendação de conteúdo em plataformas digitais, uma vez que podem ter alto poder de influência sobre os gostos e preferências dos usuários e, consequentemente, sobre sua identidade. Nesse aspecto, a explicação poderia assumir o papel de aumentar a consciência dos usuários sobre a atuação da plataforma, sendo “*integradas como um recurso padrão prontamente disponível nas recomendações, que as pessoas possam escolher revisar quando quiserem ou que apareçam como um pop-up na interface de plataformas online*” (tradução nossa).⁴⁷

Uma pesquisa feita com usuários de plataformas digitais revelou que além de desejarem ser bem informados sobre sistemas de recomendação de conteúdo, a fim de melhor proteger sua privacidade e segurança online, eles também preferiam explicações concisas e categóricas, em linguagem acessível e com elementos visuais

45. GALLI, Federico; LOREGGIA, Andrea; SARTOR, Giovanni. *The Regulation of Content Moderation. The Legal Challenges of the Fourth Industrial Revolution*, v. 57, pp. 63-87, 2023.

46. EDER, Niklas. *Making Systemic Risk Assessments Work: How the DSA Creates a Virtuous Loop to Address the Societal Harms of Content Moderation*. *German Law Journal*, v. 25, pp. 1197-1218, 2024, p. 1200.

47. FABBRI, Matteo. *Self-determination through explanation: an ethical perspective on the implementation of the transparency requirements for recommender systems set by the Digital Services Act of the European Union*. *Proceedings of the 2023 AAAI/ACM Conference on AI, Ethics, and Society*, pp. 653-661, 2023. Disponível em: <https://dl.acm.org/doi/10.1145/3600211.3604717>. Acesso em: 7 fev. 2025.

moderados.⁴⁸ Ainda, eram preferidas explicações específicas sobre por que determinado conteúdo era recomendado, e não explicações genéricas sobre como o sistema de recomendação da plataforma funcionava.⁴⁹ Este tipo de pedido também pode ser percebido em relação à moderação que opera por meio da intervenção direta em conteúdos.

De acordo com um estudo sobre as principais reclamações de usuários de redes sociais no Brasil, 54,34% são sobre o procedimento de moderação no caso de remoção de postagens e suspensão/bloqueio de contas.⁵⁰ Nesse universo, 52,46% das queixas são apenas sobre fundamentação inadequada de decisões de moderação, ou seja, sobre quais violações à política da plataforma a conta ou conteúdo derrubado efetivamente tinha incorrido. Em segundo lugar, com 22,54%, estavam as queixas sobre contestação de decisão de moderação não respondida.

Nesse sentido, pesquisadoras têm defendido a ideia de um direito ao devido processo na moderação de conteúdo, que corresponderia a um “conjunto de mecanismos e procedimentos com fim de legitimar o processo de gerenciamento do conteúdo [de terceiro] a ser disponibilizado (ou não) pelas plataformas digitais e do seu modo de exibição”.⁵¹ Dentre seus elementos, estaria a necessidade de fundamentação adequada de decisões de moderação, notificação ao usuário sobre medidas tomadas, possibilidade de recurso às decisões da plataforma e prazos procedimentais para contestação e resposta.⁵²

48. HAQUE, AKM Bahalul; ISLAM, Najmul; MIKALEF, Patrick. *To Explain or Not To Explain: An Empirical Investigation of AI-based Recommendations on Social Media Platforms*. *Electronic Markets*, v. 35, n. 2, 2025.

49. *Ibidem*.

50. SILVA, Fernanda dos Santos Rodrigues et al. *Reclamações sobre o procedimento de moderação de conteúdo em redes sociais: o que pensam os usuários*. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2024. Disponível em: <https://bit.ly/4enMVKv>. Acesso em: 7 fev. 2025.

51. SILVA, Fernanda dos Santos Rodrigues; GERTRUDES, Júlia Maria Caldeira; SILVA, Rafaela Ferreira Gonçalves da. *Regulação de plataformas e devido processo na moderação de conteúdo: perspectivas em 5 continentes*. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2024. Disponível em: <https://irisbh.com.br/publicacoes/devido-processo-na-moderacao-de-conteudo-em-5-continentes/>. Acesso em: 5 fev. 2025.

52. SILVA, Fernanda dos Santos Rodrigues; GERTRUDES, Júlia Maria Caldeira; SILVA, Rafaela Ferreira Gonçalves da. *Caixa de Ferramentas: Guia de Boas Práticas para Análise de Moderação de*

Na União Europeia, o *Digital Services Act (DSA)*, voltado a regular plataformas digitais, trouxe uma série de previsões que constituem o estabelecimento de um direito ao devido processo, ainda que não nominalmente. Normas que determinam notificação dos usuários, avaliações sobre denúncias de conteúdo nocivo, necessidade de justificação de decisões, criação de um sistema de contestação interno e externo, dentre outros, são apenas alguns exemplos nesse sentido.⁵³ Entretanto, há autores que criticam essa abordagem, por entender que ela transfere toda a responsabilidade sobre monitoramento prévio e posterior, bloqueio e remoção de conteúdo ilegal e prejudicial às plataformas, o que concederia ampla discricionariedade e a adoção de respostas simbólicas que não resolvem o problema.⁵⁴ Assim, seriam necessárias mudanças, como uma regulação que auxiliasse os provedores de aplicações a determinar o que é conteúdo nocivo e ilegal e maior participação de atores externos no processo de fiscalização.⁵⁵

No caso de sistemas algorítmicos, os direitos de informação, explicação e revisão também despontam como fundamentais para mitigação dos problemas mencionados no capítulo anterior. No caso da informação, trata-se de informar adequadamente os indivíduos quando houver interação ou uso de sistemas de IA; no caso da explicação, assim como para regulação de plataformas digitais, é o fornecimento de informações precisas sobre as razões e os processos técnicos que levaram a determinada decisão automatizada; e o direito de revisão, por sua vez, trata-se da revisão humana sobre decisões automatizadas.⁵⁶

Conteúdo. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2024. Disponível em: <https://bit.ly/467wqzh>. Acesso em: 7 fev. 2025.

53. SILVA, Fernanda dos Santos Rodrigues; GERTRUDES, Júlia Maria Caldeira; SILVA, Rafaela Ferreira Gonçalves da. *Regulação de plataformas e devido processo na moderação de conteúdo: perspectivas em 5 continentes*. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2024. Disponível em: <https://irisbh.com.br/publicacoes/devido-processo-na-moderacao-de-conteudo-em-5-continentes/>. Acesso em: 5 fev. 2025.

54. JIANG, Na; HAN, Rong. *The regulation of content moderation in the DSA: can we trust the due process?* Forensic Research & Criminology International Journal, v. 12, n. 4, pp. 231-238, 2024.

55. JIANG, Na; HAN, Rong. *The regulation of content moderation in the DSA: can we trust the due process?* Forensic Research & Criminology International Journal, v. 12, n. 4, pp. 231-238, 2024.

56. PAPAGIANNIDIS, Emmanouil; MIKALEF, Patrick; CONBOY, Kieran. *Responsible artificial intelligence governance: A review and research framework*. Journal of Strategic Information Systems,

Este último, na verdade, vai além da mera revisão: cuida-se da presença humana ao longo do processo de tomada de decisão da IA, por meio de estratégias de supervisão, monitoramento contínuo e análise detalhada após incidentes.⁵⁷ De acordo com o relatório da Comissão Europeia para uma abordagem de excelência e confiança sobre sistemas de inteligência artificial, a supervisão humana é essencial para não colocar em risco a autonomia dos indivíduos e produzir outros efeitos negativos, de modo que “*uma IA fiável, ética e centrada no ser humano só pode ser alcançado através da garantia de um envolvimento adequado dos seres humanos em aplicações de IA de alto risco*”.⁵⁸

Por fim, um importante princípio que tem sido evocado no caso de sistemas algorítmicos é o de não-discriminação, ou seja, do enfrentamento à “*inclinação ou preconceito a favor ou contra pessoas, objetos ou posições, bem como vieses inerentes em conjuntos de dados, que podem gerar resultados indesejáveis*”.⁵⁹ Este princípio é especialmente relevante diante dos casos de discriminação algorítmica já mencionados, mas deve vir acompanhado de medidas capazes de efetivá-lo na prática. No ponto, para evitar a “discriminação por padrão”, é necessário questionar até mesmo o que é considerado inovação, o que está por trás da visão idealizada de tecnologia e quais são os interesses sociais priorizados no seu desenvolvimento.⁶⁰

3.2 Medidas de governança e transparência para agentes envolvidos com moderação automatizada de conteúdo

Na seara das medidas de governança, a abordagem sistêmica em torno de riscos na regulação de plataformas tem ganhado destaque, principalmente após a

v. 34, n. 2, 2025.

57. *Ibidem*.

58. COMISSÃO EUROPEIA. *Livro Branco: sobre a inteligência artificial - Uma abordagem europeia virada para a excelência e a confiança*. Bruxelas, 19 fev. 2020. Disponível em: https://commission.europa.eu/document/download/d2ec4039-c5be-423a-81ef-b9e44e79825b_pt?file-name=commission-white-paper-artificial-intelligence-feb2020_pt.pdf. Acesso em: 7 fev. 2025.

59. PAPAGIANNIDIS, Emmanouil; MIKALEF, Patrick; CONBOY, Kieran. *Op. cit.*, p. 8.

60. BENJAMIN, Ruha. *Race after technology: abolitionist tools for the New Jim Code*. Medford, MA: Polity, 2019.

aprovação do DSA. A norma passou a prever que plataformas classificadas como de “muito grande dimensão” devem trabalhar na identificação, análise e avaliação diligente de riscos sistêmicos, considerados aqueles que decorrem do seu design ou funcionamento.⁶¹ “A execução de testes e a adaptação dos sistemas algorítmicos, incluindo os sistemas de recomendação”⁶² está entre as medidas de mitigação passíveis de serem empregadas.

Em que pese suas limitações,⁶³ a abordagem sistêmica foi reproduzida no Projeto de Lei 2.630/2020, voltado a regular plataformas digitais no Brasil. Ela chegou a ser avaliada como positiva por um coletivo de organizações da sociedade civil, que a destacou como “*um caminho mais favorável e seguro à proteção dos direitos dos usuários e usuárias, na medida em que busca resolver questões estruturais e mitigar potenciais riscos dos serviços, não se limitando a temas específicos de conteúdo*”.⁶⁴ A busca por riscos de vieses discriminatórios, portanto, poderia ser objeto desse tipo de análise.

De outra sorte, no âmbito da discussão regulatória da IA, a abordagem que tem ganhado destaque é a da gradação de riscos, que prevê a classificação de sistemas de inteligência artificial conforme o seu grau de risco à sociedade, desde os riscos mínimos até os inaceitáveis. Quanto maior o grau de risco, mais rígidas são as medidas de governança previstas. Novamente, a influência vem do contexto europeu, com a

61. EUROPEAN COMMISSION. Article 34, Risk assessment - the Digital Services Act (DSA). Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act). Disponível em: https://www.eu-digital-services-act.com/Digital_Services_Act_Article_34.html. Acesso em: 7 fev. 2025.

62. UNIÃO EUROPEIA. Regulamento (UE) 2022/2065 do Parlamento Europeu e do Conselho de 19 de outubro de 2022. Relativo a um mercado único para os serviços digitais e que altera a Diretiva 2000/31/CE (Regulamento dos Serviços Digitais). Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32022R2065>. Acesso em: 3 jul. 2024.

63. EDER, Niklas. *Making Systemic Risk Assessments Work: How the DSA Creates a Virtuous Loop to Address the Societal Harms of Content Moderation*. German Law Journal, v. 25, pp. 1197-1218, 2024.

64. COALIZÃO DIREITOS NA REDE. *A Democracia brasileira deve assumir um papel ativo na regulação das Plataformas Digitais*. 12 abr. 2023. Disponível em: <https://direitosna-rede.org.br/2023/04/12/a-democracia-brasileira-deve-assumir-um-papel-ativo-na-regulacao-das-plataformas-digitais/>. Acesso em: 7 fev. 2025.

recente aprovação do *AI Act*, que inspirou também o debate regulatório brasileiro. O Projeto de Lei 2.338/2023, à frente da regulação de IA no Brasil, chegou a prever em seu texto que sistemas de “*produção, curadoria, difusão, recomendação e distribuição, em grande escala e significativamente automatizada, de conteúdo por provedores de aplicação, com objetivo de maximização do tempo de uso e engajamento das pessoas ou grupos afetados*” deveriam ser classificados como de alto risco, no entanto, após intensa pressão do setor privado, o dispositivo foi retirado do PL antes da aprovação no plenário do Senado Federal.⁶⁵

Autores que defendem a sua inclusão no rol de sistemas de alto risco destacam justamente as falhas na moderação de conteúdo danoso ou a remoção indevida de postagens como ações que podem impactar sobremaneira direitos fundamentais, como é o caso da liberdade de expressão e direito à informação.⁶⁶ Ainda, a utilização ilícita desse tipo de sistema para censurar debates políticos ou para manipulação do debate público, por exemplo, somam-se aos motivos para reconsiderar a sua gradação de risco.⁶⁷ Com efeito, a possibilidade de modulação de comportamentos por meio de algoritmos de recomendação representa um grave risco até mesmo para o Estado democrático de direito, na medida em que pode interferir na autonomia dos cidadãos em seu processo de tomada de decisão.

Nesse contexto, ganha ainda mais relevo a sugestão de especialistas de que a moderação de conteúdo automatizada seja submetida especificamente a avaliações de impacto sobre direitos humanos,⁶⁸ o que poderia ser objeto de uma regulação de plataformas. Na regulação da IA, este tipo de instrumento pode ser melhor traduzido em avaliações de impacto algorítmico, que visam “*identificar e prever possíveis riscos*

65. LÉON, Lucas Pordeus. *Big tech é excluída do rol de Inteligência Artificial de alto risco*. Agência Brasil, 3 dez. 2024. Disponível em: <https://agenciabrasil.ebc.com.br/politica/noticia/2024-12/big-tech-e-excluida-do-rol-de-inteligencia-artificial-de-alto-risco>. Acesso em: 7 fev. 2025.

66. JIANG, Na; HAN, Rong. *The regulation of content moderation in the DSA: can we trust the due process?* Forensic Research & Criminology International Journal, v. 12, n. 4, pp. 231-238, 2024.

67. *Ibidem*.

68. SILVA, Fernanda dos Santos Rodrigues; GERTRUDES, Júlia Maria Caldeira. *Governança da moderação de conteúdo online: percepções sobre o papel dos atores e regimes*. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2023. Disponível em: <https://bit.ly/3WHMUIg>. Acesso em: 7 fev. 2025.

que uma determinada atividade pode causar a direitos e bens protegidos pelo nosso ordenamento jurídico".⁶⁹ Desse modo, possibilita a implementação de "*salvaguardas e medidas de mitigação de riscos, o que permite mitigar ou eliminar os impactos deletérios dessa atividade a um nível aceitável*".⁷⁰ É uma ferramenta que poderia contribuir para a identificação prévia de vieses em sistemas de moderação de conteúdo, visando evitar problemas futuros.

Outra importante ferramenta referida pela literatura é a obrigatoriedade de elaboração e publicação de relatórios de transparência. Na falta de diretrizes mínimas, as plataformas têm elaborado seus relatórios com foco nos pontos que entendem mais importantes. Estudos apontam, inclusive, que há uma tendência de que as informações sejam mais detalhadas em relação a decisões de moderação determinadas por agentes estatais, como por meio de ações judiciais, do que sobre práticas internas de moderação.⁷¹ No entanto, isso não contribui para uma transparência significativa, pois ainda mantém obscuro o cenário em torno da atuação dos próprios intermediários.

Com uma previsão legal que exija uma série de informações mínimas, desde números e razões para decisões de moderação até o nível de investimento e composição de equipes de moderação espalhadas pelo globo, esses documentos podem contribuir para identificar a fonte de problemas na análise de contexto e de línguas específicas. Em que pese considerações devam ser feitas acerca da nocividade da profissão de moderador humano, a ausência de investimentos adequados para análises em outros idiomas que não o inglês e times de moderação mais enxutos em países que não os Estados Unidos, por exemplo, podem contribuir para um maior índice de falha nesses casos.⁷² A esse respeito, especialistas recomendam também que as equipes sejam

69. LEMOS, Alessandra; BUARQUE, Gabriela; SOARES, Ingrid; MULIN, Victor; CHIAVONE, Tayrone. *Relatório de Avaliação de Impacto Algorítmico para a proteção dos direitos fundamentais*. Brasília: Laboratório de Políticas Públicas e Internet, 2023, p. 21.

70. *Ibidem*.

71. URMAN, Aleksandra. MAKHORTYKH, Mykola. *How transparent are transparency reports? Comparative analysis of transparency reporting across online platforms*. Telecommunications Policy, v. 47, n. 3, abr./2023. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0308596122001793>. Acesso em: 2 jul. 2024.

72. VIANNA, Rodolfo. "*Eles temem ser transparentes*", diz Frances Haugen sobre o Facebook.

melhor instruídas acerca de contextos e especificidades locais,⁷³ o que pode ajudar para uma supervisão humana mais acurada sobre o funcionamento da moderação de conteúdo.

Na seara da IA, estudos apontam que indivíduos de grupos minoritários teriam maior empatia com questões relacionadas a discriminação, corroborando a necessidade de se debater uma maior diversidade na área.⁷⁴ Em razão disso, seria importante a adoção de medidas como treinamento de profissionais de software acerca dos impactos sociais da tecnologia, o aumento da diversidade de equipes e a criação de comitês de equidade, diversidade e inclusão com profissionais de software com diferentes marcadores sociais.⁷⁵ Este cenário poderia contribuir para que, desde seu desenvolvimento, sistemas automatizados de moderação fossem construídos com maior sensibilidade a questões de discriminação tanto direta quanto indireta.

4 CONCLUSÃO

Após uma década, o Marco Civil da Internet passou a ser mais intensamente discutido, seja em âmbito político como jurídico, diante de sua evidente necessidade de atualização. Embora ainda não haja conclusão pela inconstitucionalidade de um ou outro de seus dispositivos, é fato que o seu silêncio sobre a forma com que plataformas devem conduzir seus processos de moderação de conteúdo não encontra mais lugar em um cenário onde as chamadas *big techs* adquirem cada vez mais poder econômico e as pessoas utilizam as redes sociais, inclusive, como fonte de informação.

Desinformante*, 4 jul. 2022. Disponível em: <https://desinformante.com.br/eles-temem-ser-transparentes-diz-frances-haugen-sobre-o-facebook/>. Acesso em: 2 jul. 2024.

73. SILVA, Fernanda dos Santos Rodrigues; GERTRUDES, Júlia Maria Caldeira. *Governança da moderação de conteúdo online: percepções sobre o papel dos atores e regimes*. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2023, p. 29. Disponível em: <https://bit.ly/3WHMUIg>. Acesso em: 17 jun. 2024.

74. SANTOS, Ronnie de Souza; LIMA, Luiz Fernando de. MAGALHÃES, Cleyton. *The Perspective of Software Professionals about Algorithmic Racism*. In: International Symposium on Empirical Software Engineering and Measurement, ESEM, 2023, New Orleans. Proceedings [...] New Orleans: Association for Computing Machinery, 2023. Disponível em: <https://arxiv.org/pdf/2306.15133.pdf>. Acesso em: 31 jan. 2024.

75. *Ibidem*.

Se há dez anos o gerenciamento de conteúdo era uma discussão mais secundária na definição de uma regulação civil para a internet, hoje ele tomou o centro dos debates, ainda mais com o registro de centenas de milhares de informações sendo compartilhadas em diferentes plataformas por minuto. A partir da criação de tecnologias aptas a ajudar a moderar todo esse conteúdo, surgem desafios com significativo impacto em direitos fundamentais, em virtude dos riscos e limitações dessas ferramentas. Falhas na análise de contexto e detecção de idiomas e dialetos, vieses discriminatórios, falta de transparência e explicabilidade, modulação de comportamento dos usuários e impactos sobre o debate público são alguns dos principais exemplos a serem mencionados.

Considerando, porém, que a moderação de conteúdo por IA reúne, pelo menos, duas discussões, como a regulação de sistemas algorítmicos e de plataformas digitais, o presente artigo buscou analisar os principais pontos de convergência entre ambos os diplomas legais, para fins do enfrentamento dos desafios relacionados à moderação de conteúdo automatizada. A partir da investigação, foi possível identificar que uma série de medidas de mitigação podem ser adotadas nas duas regulações de modo complementar. Na seara dos direitos, o destaque vai para o direito à explicação, informação e revisão, que juntos contribuem para que os usuários possam compreender e questionar decisões de moderação. O princípio da não-discriminação nesse contexto auxilia enquanto norteador de medidas que possam efetivá-lo concretamente, de modo a impedir a exclusão de grupos vulnerabilizados do espaço digital.

Quanto às medidas de governança, as avaliações de impacto algorítmico para IA e de riscos sistêmicos e impacto sobre direitos humanos para plataformas digitais se complementam enquanto instrumentos de antecipação de problemas e soluções. Por outro lado, tanto a previsão legal de incentivos para equipes de desenvolvimento de sistemas algorítmicos mais diversas, quanto de times de moderação de conteúdo melhor instruídos sobre contextos locais reforçam que o elemento humano por trás da máquina é componente fundamental para o seu funcionamento adequado.

Ainda que todas as ações acima, em maior ou menor grau, digam respeito a aumentar a transparência e explicabilidade perante a moderação automatizada, a obrigação de elaboração de relatórios de transparência mais robustos e completos desponta como essencial para fornecer mais informações ao usuário sobre quais têm sido os esforços empregados por plataformas digitais, bem como de que forma isso

tem acontecido.

Por fim, as abordagens de gradação de risco para sistemas de IA e de avaliação de riscos sistêmicos para plataformas digitais representam, em conjunto, uma forma de manter maior *accountability* tanto sob a perspectiva de desenvolvimento dos sistemas, quanto sob de sua operação. Este parece ser o ponto-chave, isto é, a atuação em mais de uma frente é o que sustenta que a regulação da IA e de plataformas digitais devem, sim, seguir caminhos diferentes, não só porque tratam de objetos distintos, ainda que correlatos, mas porque sua aplicação associada pode promover uma moderação de conteúdo mais confiável e transparente.

REFERÊNCIAS

- ALVES, Marco Antônio Sousa. *A resistência à governamentalidade algorítmica: condutas e contracondutas na era da informação*. In: MATOS, Andityas Soares de Moura Costa (org.). *Ensaio de desobediência epistemocrítica: dimensões antagonistas na era das sujeições bio-político-cibernéticas*. Belo Horizonte: Initia Via, 2019.
- BENJAMIN, Ruha. *Race after technology: abolitionist tools for the New Jim Code*. Medford, MA: Polity, 2019.
- BLOCH-WEBB, Hannah. *Automation in Moderation*. Cornell International Law Journal, v. 53, 2020, pp. 41-96, p. 48. Disponível em: <https://community.lawschool.cornell.edu/wp-content/uploads/2021/03/Bloch-Wehba-final.pdf>. Acesso em: 17 jun. 2024.
- BRASIL. Câmara dos Deputados. *Projeto de Lei nº 21, de 2020*. Estabelece fundamentos, princípios e diretrizes para o desenvolvimento e a aplicação da inteligência artificial no Brasil; e dá outras providências. Brasília, DF: Câmara dos Deputados, 2020. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=9063365&ts=1656528542410&disposition=inline>. Acesso em: 2 jul. 2024.
- BRASIL. *Lei nº 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 2 jul. 2024.
- BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 2 jul. 2024.
- BRASIL. Senado Federal. *Projeto de Lei nº 2.338, de 2023*. Dispõe sobre o uso da inteligência artificial. Brasília, DF: Senado Federal, 2023, p. 3. Disponível em: <https://legis.senado.leg.br/sdleg->

getter/documento?dm=9347622&ts=1684441712955&disposition=in-line&_gl=1*1rfx39i*_ga*MTU0ODcx-NzM1NjY4xNjg3OTU4MjIx*_ga_CW3ZH25XMK*MTY4ODY0MTMxOS4xMS4xLjE2ODg2NDMwODkuMC4wLjA. Acesso em: 05 jul. 2023.

BRASIL. Senado Federal. *Relatório ao Projeto de Lei 2.338/2023, de autoria do Senador Eduardo Gomes*. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento/download/9652e2f1-baa4-4bbe-98a9-2ee4abcc64df>. Acesso em: 3 jul. 2024.

CETIC.BR. *Acesso à internet no Brasil: desafios para conectar toda a população*. Panorama Setorial da Internet, ano 8, n. 1, mar./2016. Disponível em: https://cetic.br/media/docs/publicacoes/6/Panorama_Setorial_11.pdf. Acesso em: 15 jun. 2024.

COALIZÃO DIREITOS NA REDE. *A Democracia brasileira deve assumir um papel ativo na regulação das Plataformas Digitais*. 12 abr. 2023. Disponível em: <https://direitosna-rede.org.br/2023/04/12/a-democracia-brasileira-deve-assumir-um-papel-ativo-na-regulacao-das-plataformas-digitais/>. Acesso em: 7 fev. 2025.

COMISSÃO EUROPEIA. *Livro Branco: sobre a inteligência artificial - Uma abordagem europeia viável para a excelência e a confiança*. Bruxelas, 19 fev. 2020. Disponível em: https://commission.europa.eu/document/download/d2ec4039-c5be-423a-81ef-b9e44e79825b_pt?file-name=commission-white-paper-artificial-intelligence-feb2020_pt.pdf. Acesso em: 7 fev. 2025.

CRUZ, Francisco Brito. *Inteligência artificial e internet: um olhar sobre o conteúdo de usuários e a sua moderação*. Revista USP, São Paulo, n. 141, pp. 65-80, abr./mai./jun. 2024. Disponível em: <https://jornal.usp.br/wp-content/uploads/2024/05/5-Francisco-Cruz.pdf>. Acesso em: 2 jul. 2024.

DINIZ, Maria Helena. *A antinomia real e a polêmica do diálogo das fontes*. Revista Jurídica, v. 3, n. 56, Curitiba, 2019, pp. 228-247. Disponível em: <https://revista.unicuritiba.edu.br/index.php/RevJur/article/download/3575/371371967>. Acesso em: 3 jul. 2024.

DOMO. *Data never sleeps 10.0*. Disponível em: <https://web-assets.domo.com/miyagi/images/product/product-feature-22-data-never-sleeps-10.png>. Acesso em: 17 jun. 2024.

EDER, Niklas. *Making Systemic Risk Assessments Work: How the DSA Creates a Virtuous Loop to Address the Societal Harms of Content Moderation*. German Law Journal, v. 25, pp. 1197-1218, 2024.

ELECTRONIC FRONTIER FOUNDATION. Section 230. Disponível em: <https://www.eff.org/pt-br/issues/cda230>. Acesso em: 2 jul. 2024.

EUROPEAN COMISSION. *Article 34, Risk assessment - the Digital Services Act (DSA)*. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act). Disponível em: https://www.eu-digital-services-act.com/Digital_Services_Act_Article_34.html. Acesso em: 7 fev. 2025.

FABBRI, Matteo. *Self-determination through explanation: an ethical perspective on the*

- implementation of the transparency requirements for recommender systems set by the Digital Services Act of the European Union*. Proceedings of the 2023 AAAI/ACM Conference on AI, Ethics, and Society, pp. 653-661, 2023. Disponível em: <https://dl.acm.org/doi/10.1145/3600211.3604717>. Acesso em: 7 fev. 2025.
- FARID, Hany. *An Overview of Perceptual Hashing*. Journal of Online Trust and Safety, v. 1, n. 1, 2021. Disponível em: <https://tsjournal.org/index.php/jots/article/view/24>. Acesso em: 2 jul. 2024.
- FERREIRA, Sérgio Rodrigo da Silva. *Repensar a esfera pública política a partir das Câmaras de Eco: conceitos e questões metodológicas*. Liinc em Revista, Rio de Janeiro, v. 18, n. 2, e6067, nov.2022. Disponível em: <https://revista.ibict.br/liinc/article/view/6067/5694>. Acesso em: 17 jun. 2024.
- GALLI, Federico; LOREGGIA, Andrea; SARTOR, Giovanni. *The Regulation of Content Moderation. The Legal Challenges of the Fourth Industrial Revolution*, v. 57, pp. 63-87, 2023.
- GANDRA, Alana. *Moradores do asfalto têm visão preconceituosa de favelas, mostra pesquisa*. Agência Brasil, 16 fev. 2015. Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2015-02/moradores-do-asfalto-tem-visao-preconceituosa-em-relacao-favelas>. Acesso em: 2 jul. 2024.
- GOMES, Alessandra. ANTONIALLI, Dennys. OLIVA, Thiago. *Drag queens e Inteligência Artificial: computadores devem decidir o que é 'tóxico' na internet?* InternetLab, 28 jun. 2019. Disponível em: <https://internetlab.org.br/pt/noticias/drag-queens-e-inteligencia-artificial-computadores-devem-decidir-o-que-e-toxico-na-internet/>. Acesso em: 16 jun. 2024.
- GRAY, Kishonna L. STEIN, Krysten. *"We 'said her name' and got zucked": Black Women calling-out the carceral logics of digital platforms*. Gender & Society, v. 35, n. 4, ago./2021, pp. 538-545. Disponível em: <https://journals.sagepub.com/doi/pdf/10.1177/08912432211029393>. Acesso em: 16 jun. 2024.
- HAIMSON, Oliver et al. *Disproportionate Removals and Differing Content Moderation Experiences for Conservative, Transgender, and Black Social Media Users: Marginalization and Moderation Gray Areas*. Proceedings of the ACM on Human-Computer Interaction, v. 5, n. 466pp 1–35, out./2021. Disponível em: <https://dl.acm.org/doi/10.1145/3479610>. Acesso em: 16 jun. 2024.
- HAQUE, AKM Bahalul; ISLAM, Najmul; MIKALEF, Patrick. *To Explain or Not To Explain: An Empirical Investigation of AI-based Recommendations on Social Media Platforms*. Electronic Markets, v. 35, n. 2, 2025.
- JIANG, Na; HAN, Rong. *The regulation of content moderation in the DSA: can we trust the due process?* Forensic Research & Criminology International Journal, v. 12, n. 4, pp. 231-238, 2024.
- KREMER, Bianca. *Racismo algorítmico*. Rio de Janeiro: CESeC, 2023.
- LEE, Edward. *Moderating Content Moderation: A Framework for Nonpartisanship in Online Governance*. American University Law Review, v. 70, n. 03, p. 913-1060, fev. 2021.
- LEE, Nicol Turner. *Detecting racial bias in algorithms and machine learning*. Journal of Information, Communication and Ethics in Society, v. 16, n. 3, pp. 252-260. Disponível em:

- <https://www.emerald.com/insight/content/doi/10.1108/JICES-06-2018-0056/full/html>. Acesso em: 2 jul. 2024.
- LEMOS, Alessandra; BUARQUE, Gabriela; SOARES, Ingrid; MULIN, Victor; CHIAVONE, Tayrone. Relatório de Avaliação de Impacto Algorítmico para a proteção dos direitos fundamentais. Brasília: Laboratório de Políticas Públicas e Internet, 2023.
- LÉON, Lucas Pordeus. *Big tech é excluída do rol de Inteligência Artificial de alto risco*. Agência Brasil, 3 dez. 2024. Disponível em: <https://agenciabrasil.ebc.com.br/politica/noticia/2024-12/big-tech-e-excluida-do-rol-de-inteligencia-artificial-de-alto-risco>. Acesso em: 7 fev. 2025.
- LIRA, Isadora. *(In)visibilidades na rede: discurso de ódio e censura das plataformas*. Le Monde Diplomatique Brasil. 25 mai. 2022. Disponível em: <https://diplomatique.org.br/invisibilidades-na-rede-discurso-de-odio-e-censura-das-plataformas/>. Acesso em: 2 jul. 2024.
- MARQUES, Claudia Lima. *Superação das antinomias pelo diálogo das fontes: o modelo brasileiro de coexistência entre o Código de Defesa do Consumidor e o Código Civil de 2002*. Revista da Escola Superior da Magistratura de Sergipe, n. 7, 2004. Disponível em: <https://core.ac.uk/download/pdf/79073279.pdf>. Acesso em: 3 jul. 2024.
- META. *Community Standards Enforcement Report: hate speech*. Disponível em: <https://transparency.meta.com/reports/community-standards-enforcement/hate-speech/instagram/>. Acesso em: 17 jun. 2024.
- META. *Community Standards Enforcement Report: violence and incitement*. Disponível em: <https://transparency.meta.com/reports/community-standards-enforcement/violence-incitement/instagram/>. Acesso em: 17 jun. 2024.
- META. *Facebook Community Standards: hate speech*. Disponível em: https://transparency.meta.com/pt-br/policies/community-standards/hate-speech/?source=https%3A%2F%2Fwww.facebook.com%2Fcommunitystandards%2Fhate_speech. Acesso em: 16 jun. 2024.
- NEWMAN, Nic et al. *Digital News Report 2024*. Oxford: Reuters Institute, University of Oxford, 2024. Disponível em: <https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2024-06/DNR%202024%20Final%20lo-res-compressed.pdf>. Acesso em: 17 jun. 2024.
- NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR (ed.). *Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros: TIC Domicílios 2022* [livro eletrônico]. São Paulo: Comitê Gestor da Internet no Brasil, 2023. Disponível em: https://www.ce-tic.br/media/docs/publicacoes/2/20230825143720/tic_domicilios_2022_livro_eletronico.pdf. Acesso em: 15 jun. 2024.
- PACETE, Luiz Gustavo. *Brasil é o terceiro maior consumidor de redes sociais em todo o mundo*. Forbes, Forbes Tech, 9 mar. 2023. Disponível em: <https://forbes.com.br/forbes-tech/2023/03/brasil-e-o-terceiro-pais-que-mais-consome-redes-sociais-em-todo-o-mundo/>. Acesso em: 15 jun. 2024.

- PAPAGIANNIDIS, Emmanouil; MIKALEF, Patrick; CONBOY, Kieran. *Responsible artificial intelligence governance: A review and research framework*. Journal of Strategic Information Systems, v. 34, n. 2, 2025.
- PREM, Erich. KRENN, Brigitte. *On Algorithmic Content Moderation*. In: WERTHNER, Hannes. *Introduction to Digital Humanism: a textbook*. Cham: Springer, 2024, p. 481. Disponível em: https://link.springer.com/chapter/10.1007/978-3-031-45304-5_30. Acesso em: 16 jun. 2024.
- RIMER, K; PETER, S. Algorithmic audiencing: *Why we need to rethink free speech on social media*. Research Paper, Australia, v. 36, 4, p. 409-426, dez, 2021. Disponível em: <https://ses.library.usyd.edu.au/bitstream/handle/2123/25053/publisher%20author%20accepted%20manuscript.pdf?sequence=1&isAllowed=y>. Acesso em: 17 jun. 2024.
- ROBERTS, Sarah T. *Digital detritus: 'Error' and the logic of opacity in social media content moderation*. First Monday, v. 23 n. 3 mar. 2018. Disponível em: <https://firstmonday.org/ojs/index.php/fm/article/view/8283/6649>. Acesso em: 16 jun. 2024.
- ROUVROY, Antoinette; BERNS, Thomas. *Governamentalidade algorítmica e perspectivas de emancipação: o dispar como condição de individuação pela relação?* In: BRUNO, Fernanda et al. *Tecnopolíticas da vigilância: perspectivas da margem*. São Paulo: Boitempo, 2018.
- SANTOS, Ronnie de Souza; LIMA, Luiz Fernando de. MAGALHÃES, Cleyton. *The Perspective of Software Professionals about Algorithmic Racism*. In: International Symposium on Empirical Software Engineering and Measurement, ESEM, 2023, New Orleans. Proceedings [...] New Orleans: Association for Computing Machinery, 2023. Disponível em: <https://arxiv.org/pdf/2306.15133.pdf>. Acesso em: 31 jan. 2024.
- SAP, Maarten. et al. *The Risk of Racial Bias in Hate Speech Detection*. Proceedings of the 57th Annual Meeting of the Association for Computational Linguistics, pp. 1668–1678, Florence, Italy, July 28 - August 2, 2019. Association for Computational Linguistics. Disponível em: <https://maarten-sap.com/pdfs/sap2019risk.pdf>. Acesso em: 2 jul. 2024.
- SENADO FEDERAL. Comissão Temporária Interna sobre Inteligência Artificial no Brasil. Disponível em: <https://legis.senado.leg.br/comissoes/comissao?codcol=2629>. Acesso em: 3 jul. 2024.
- SHENG, Chuyi. *Automated Content Moderation*. Georgetown Law Technology Review, v. 06, n. 01, p. 351-363, Jun. 2022.
- SILVA, Fernanda dos Santos Rodrigues. et al. *Marco Legal da Inteligência Artificial: Contribuições do IRIS à Comissão de Juristas do Senado*. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2021. Disponível em: <https://irisbh.com.br/wp-content/uploads/2022/06/Marco-Legal-da-Inteligencia-Artificial-Contribicoes-do-IRIS-a-Comissao-de-Juristas-do-Senado-1.pdf>. Acesso em: 3 jul. 2024.
- SILVA, Fernanda dos Santos Rodrigues et al. *Reclamações sobre o procedimento de moderação de conteúdo em redes sociais: o que pensam os usuários*. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2024. Disponível em: <https://bit.ly/4enMVKv>. Acesso em: 7 fev. 2025.

- SILVA, Fernanda dos Santos Rodrigues; GERTRUDES, Júlia Maria Caldeira. Governança da moderação de conteúdo online: percepções sobre o papel dos atores e regimes. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2023, p. 29. Disponível em: <https://bit.ly/3WHMUIg>. Acesso em: 17 jun. 2024.
- SILVA, Fernanda dos Santos Rodrigues; GERTRUDES, Júlia Maria Caldeira; SILVA, Rafaela Ferreira Gonçalves da. *Caixa de Ferramentas: Guia de Boas Práticas para Análise de Moderação de Conteúdo*. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2024. Disponível em: <https://bit.ly/467wqzh>. Acesso em: 7 fev. 2025.
- SILVA, Fernanda dos Santos Rodrigues; GERTRUDES, Júlia Maria Caldeira; SILVA, Rafaela Ferreira Gonçalves da. *Regulação de plataformas e devido processo na moderação de conteúdo: perspectivas em 5 continentes*. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2024, p. 10. Disponível em: <https://irisbh.com.br/publicacoes/devido-processo-na-moderacao-de-conteudo-em-5-continentes/>. Acesso em: 15 jun. 2024.
- SUZOR, Nicolas P. et al. *What Do We Mean When We Talk About Transparency? Toward Meaningful Transparency in Commercial Content Moderation*. International Journal of Communication, v. 13, 2019, pp. 1526-1543. Disponível em: <https://ijoc.org/index.php/ijoc/article/view/9736>. Acesso em: 2 jul. 2024.
- UNIÃO EUROPEIA. *Regulamento (UE) 2022/2065 do Parlamento Europeu e do Conselho de 19 de outubro de 2022*. Relativo a um mercado único para os serviços digitais e que altera a Diretiva 2000/31/CE (Regulamento dos Serviços Digitais). Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32022R2065>. Acesso em: 3 jul. 2024.
- URMAN, Aleksandra. MAKHORTYKH, Mykola. *How transparent are transparency reports? Comparative analysis of transparency reporting across online platforms*. Telecommunications Policy, v. 47, n. 3, abr./2023. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0308596122001793>. Acesso em: 2 jul. 2024.
- VALENTE, Jonas. *Tecnologia, informação e poder: das plataformas online aos monopólios digitais*. Tese (Doutorado em Sociologia) – Universidade de Brasília, Brasília, 2019, 399p.
- VALENTE, Mariana. *Direito autoral e plataformas de internet: um assunto aberto*. InternetLab, 18 abr. 2019. Disponível em: <https://internetlab.org.br/pt/especial/direito-autoral-e-plataformas-de-internet-um-assunto-em-aberto/>. Acesso em: 17 jun. 2024.
- VIANNA, Rodolfo. “*Eles temem ser transparentes*”, diz Frances Haugen sobre o Facebook. *Desinformante**, 4 jul. 2022. Disponível em: <https://desinformante.com.br/eles-temem-ser-transparentes-diz-frances-haugen-sobre-o-facebook/>. Acesso em: 2 jul. 2024.

A (IN)CONSTITUCIONALIDADE DO ART. 19 DO MARCO CIVIL DA INTERNET

Natália Cristina Chaves

Mestre e Doutora em Direito Empresarial pela UFMG. Professora da Graduação e do Programa de Pós-Graduação em Direito da UFMG. Sócia fundadora da Passos e Chaves Sociedade de Advogados.

Helena Penna Marchi

Mestranda em Direito pela UFMG. Advogada.

DOI: <https://doi.org/10.59224/dti7.ch10>

Resumo: O Marco Civil da Internet estabeleceu, em seu artigo 19, que os provedores de aplicações de internet serão responsabilizados civilmente por conteúdo gerado por terceiros apenas quando se abstiverem de agir em face de ordem judicial expressa de remoção do conteúdo ilícito. Analisa-se o julgamento de (in)constitucionalidade do referido artigo pelo Supremo Tribunal Federal para, ao final, concluir-se que, admitida a sua inconstitucionalidade, a adoção de um modelo geral, amparado no sistema de *notice and take down*, proporciona maior resguardo aos direitos e às garantias constitucionais em evidência.

Palavras-chave: responsabilidade civil, provedores de internet, notificação.

Abstract: Article 19 of the Brazilian Marco Civil da Internet establishes that internet providers will only be held responsible for content generated by third parties when they fail to act in the event of an express court order to remove the illegal content. The Supreme Court's assessment of the (in)constitutionality of this provision is analyzed to conclude that, if its unconstitutionality is admitted, the adoption of a general model, based on the notice and take down system, provides greater protection for the constitutional rights in evidence.

Keywords: civil liability, internet providers, notification.

SUMÁRIO: 1. Introdução; 2. O modelo de *notice and take down*; 3. O modelo de *notice and stay down*; 4. A responsabilidade civil dos provedores de aplicações no Marco Civil da Internet; 5. O julgamento da matéria pelo Supremo Tribunal Federal; 6. Conclusão; Referências.

1. INTRODUÇÃO

Uma das características intrínsecas à internet e às novas tecnologias é a dinamicidade e a rapidez com que evoluem, modernizando e facilitando o acesso aos usuários em um nível global. Com essa evolução e inovação constantes, surge também a necessidade de uma contínua regulação de seus efeitos, tendo o poder legislativo o árduo dever de criar normas que acompanhem esse movimento.

Nesse contexto, as plataformas mediadas por algoritmos tornaram-se o *locus* de atividades econômicas e sociais, estabelecendo, na ausência de normas jurídicas, as regras para atuação nesses ambientes. Sob esse prisma, elas desempenham um papel importante autorregulador.

Em 2014, após anos sem regulação específica acerca da matéria, foi promulgada, no Brasil, a Lei n. 12.965/2014, conhecida como o Marco Civil da Internet que, em 2024, completou 10 anos de vigência. A Lei em comento prevê a consolidação de entendimentos firmados ao longo dos anos e teve, como um de seus objetivos, servir de base para o desenvolvimento tecnológico no território nacional.¹

Em relação à veiculação de conteúdo ilícito elaborado por terceiros, o referido diploma legal estabeleceu, em seu artigo 19,² que os provedores de aplicações de

1. SOUZA, Carlos Afonso; LEMOS, Ronaldo. *Marco civil da internet: construção e aplicação*. Juiz de Fora: Editor Editora Associada Ltda, 2016. p. 47.

2. O art. 19 da Lei 12.965/2014 assim preceitua: “Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário. § 1º A ordem judicial de que trata o *caput* deverá conter, sob pena de nulidade, identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material. § 2º A aplicação do disposto neste artigo para infrações a direitos de autor ou a direitos conexos depende de previsão legal específica, que deverá respeitar a liberdade de expressão e demais garantias previstas no art. 5º da Constituição Federal. § 3º As causas que versem sobre ressarcimento por danos decorrentes de conteúdos disponibilizados na internet relacionados à honra, à reputação ou a direitos de personalidade, bem como sobre a indisponibilização desses conteúdos por provedores de aplicações de internet, poderão ser apresentadas perante os juizados especiais. § 4º O juiz, inclusive no procedimento previsto no § 3º, poderá antecipar, total ou parcialmente, os efeitos da tutela pretendida no pedido inicial, existindo prova

internet³ serão civilmente responsabilizados apenas em face de omissão quanto à determinação judicial para a remoção do conteúdo ilícito do ar.

Em outras palavras, dito Texto legal prevê que, diante da violação dos direitos pela veiculação de material ilícito, caberá ao ofendido a provocação do Poder Judiciário para que, só então, seja possível a determinação de remoção do conteúdo, mesmo que flagrantemente ilícito. Em adição, a responsabilidade civil do provedor de aplicações de internet incidirá, exclusivamente, quando, diante de determinação judicial, ele deixar de agir para coibir o ato ilícito.

De acordo com a previsão legal, abre-se espaço para a aplicação de uma categoria subjetiva e solidária de responsabilidade civil, devendo, para tanto, ser preenchidos os requisitos elencados, a saber, a determinação judicial e a omissão do agente (provedor de aplicações de internet), nos casos de veiculação de conteúdo ilícito.

Tal dispositivo legal gerou controvérsia, principalmente em decorrência do ônus que impõe ao ofendido e da possível ineficácia da medida de remoção do conteúdo ilícito apenas mediante determinação judicial, em razão da inegável dinamicidade dos sistemas de internet. O debate chegou ao Supremo Tribunal Federal, que enfrentou, sob a sistemática de julgamento de recursos repetitivos, a discussão acerca da constitucionalidade do disposto no artigo 19 da Lei n. 12.965/2014.

Dois são os temas de repercussão geral ligados à matéria, no Supremo Tribunal Federal. O primeiro deles é o Tema de Repercussão Geral nº 987, em que se discutiu a constitucionalidade da exigência de prévia e específica ordem judicial de exclusão

inequívoca do fato e considerado o interesse da coletividade na disponibilização do conteúdo na internet, desde que presentes os requisitos de verossimilhança da alegação do autor e de fundado receio de dano irreparável ou de difícil reparação”. BRASIL. *Lei n. 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União de 24.04.2014, Brasília, DF. Disponível em <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>, acesso em: 29 dez. 2024.

3. O Marco Civil da Internet divide os provedores de internet em duas categorias, os provedores de conexão de internet e os provedores de aplicações de internet. Nos termos do art. 5º, V, da dita legislação, a conexão de internet é “a habilitação de um terminal para envio e recebimento de pacotes de dados pela internet, mediante a atribuição ou autenticação de um endereço IP”, ao passo que, nos termos do inciso VII do mesmo dispositivo legal, as aplicações de internet correspondem ao “conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet”.

de conteúdo para a responsabilização civil de provedor de internet, website e gestores de aplicativos de redes sociais por danos decorrentes dos atos ilícitos praticados por terceiros.⁴

O segundo é o Tema de Repercussão Geral nº 533, que diz respeito à controvérsia que se originou anteriormente ao Marco Civil da Internet, quando ainda não existia regulação específica acerca da matéria. Tal Tema é ligado ao dever de empresa hospedeira de sítio na internet de fiscalizar o conteúdo publicado e de retirá-lo do ar quando considerado ofensivo, sem intervenção do Judiciário.⁵

Como ambos os Temas tangenciam a questão da responsabilização dos provedores de internet por conteúdo ilícito não excluído, o julgamento deles foi realizado em conjunto, tendo se encerrado em 26 de junho de 2025.

A discussão travada no Supremo Tribunal Federal girou em torno da constitucionalidade do dispositivo que, em proteção aos direitos de liberdade de expressão e de manifestação, consagrados nos incisos II, IV, IX, XIV e XXXVI do artigo 5º e §§1º e 2º do artigo 220 da Constituição brasileira⁶, poderá implicar violação a outros direitos constitucionalmente garantidos, tais como os direitos constitucionais da

-
4. BRASIL. Supremo Tribunal Federal. *Tema 987*. Disponível em: <<https://portal.stf.jus.br/jurisprudenciaRepercussao/verAndamentoProcesso.asp?incidente=5160549&numeroProcesso=1037396&classeProcesso=RE&numeroTema=987>>, acesso em: 30 dez. 2024.
 5. BRASIL. Supremo Tribunal Federal. *Tema 533*. Disponível em: <<https://portal.stf.jus.br/jurisprudenciarepercussao/verAndamentoProcesso.asp?incidente=5217273&numeroProcesso=1057258&classeProcesso=RE&numeroTema=533>>, acesso em: 30 dez. 2024.
 6. Referidos dispositivos estabelecem: “Art. 5º. [...] II - ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei; [...] IV - é livre a manifestação do pensamento, sendo vedado o anonimato; [...] IX - é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença; [...] XIV - é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional; [...] XXXVI - a lei não prejudicará o direito adquirido, o ato jurídico perfeito e a coisa julgada; [...]”. “Art. 220. [...] §1º. Nenhuma lei conterá dispositivo que possa constituir embaraço à plena liberdade de informação jornalística em qualquer veículo de comunicação social, observado o disposto no art. 5º, IV, V, X, XIII e XIV. §2º. É vedada toda e qualquer censura de natureza política, ideológica e artística. [...]”. (BRASIL. *Constituição da República Federativa do Brasil de 1988*. Diário Oficial da União de 05.10.1988, Brasília, DF. Disponível em <https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>, acesso em: 29 dez. 2024).

personalidade (artigo 5º, X, da Constituição brasileira)⁷, do Estado Democrático de Direito (artigo 1º da Constituição brasileira)⁸ e do direito de autor (artigo 5º, XXVII e XXVIII da Constituição brasileira).⁹

Com efeito, ao responsabilizar os provedores de internet pela veiculação de conteúdo ilícito tão somente naquelas hipóteses em que se abstiverem de cumprir ordem judicial específica, resguardando, dessa forma, a liberdade de expressão assegurada constitucionalmente, o art. 19 do Marco Civil da Internet acaba por permitir o prolongamento temporal da ofensa ao direito da parte lesada e, com isso, conduz a uma possível afronta aos direitos da personalidade e, por conseguinte, à Constituição de 1988.

A discussão sobre o tema no Supremo Tribunal Federal ainda perpassou pela proteção aos direitos de autor e ao próprio Estado Democrático de Direito. Quanto a este último ponto, vale registrar que a vinculação da responsabilização de provedores de internet ao descumprimento de ordem judicial de exclusão de conteúdo ilícito possibilita a perpetuação, no tempo, das *fakes news*, ampliando-se o seu potencial de circulação e de lesão, o que pode abalar os *valores supremos de uma sociedade fraterna, pluralista e sem preconceitos, fundada na harmonia social e comprometida, na ordem interna e internacional, com a solução pacífica das controvérsias*.¹⁰

7. O art. 5º, inciso X, do Texto constitucional dispõe: “Art. 5º. [...] são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; [...]”.

8. O *caput* do art. 1º da Constituição brasileira de 1988 dispõe que: “A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito e tem como fundamentos: [...]”.

9. Tais dispositivos preceituam: “Art. 5º. [...] XXVII - aos autores pertence o direito exclusivo de utilização, publicação ou reprodução de suas obras, transmissível aos herdeiros pelo tempo que a lei fixar; XXVIII - são assegurados, nos termos da lei: a) a proteção às participações individuais em obras coletivas e à reprodução da imagem e voz humanas, inclusive nas atividades desportivas; b) o direito de fiscalização do aproveitamento econômico das obras que criarem ou de que participarem aos criadores, aos intérpretes e às respectivas representações sindicais e associativas; [...]”.

10. Nesse sentido, o preâmbulo do Texto constitucional de 1988: “Nós, representantes do povo brasileiro, reunidos em Assembléia Nacional Constituinte para instituir um Estado Democrático, destinado a assegurar o exercício dos direitos sociais e individuais, a liberdade, a segurança, o bem-estar, o desenvolvimento, a igualdade e a justiça como valores supremos de uma sociedade

A controvérsia ganha força quando analisados os modelos de *notice and take down* e *notice and stay down*. O primeiro prevê que, uma vez notificados pelo ofendido, os provedores que veiculem conteúdo gerado por terceiro deverão retirar o conteúdo do ar, sob pena de serem solidariamente responsabilizados. O segundo é utilizado especialmente para o direito de autor na União Europeia e prevê que, uma vez cientificados acerca do conteúdo ilícito, os provedores deverão empregar esforços para, além de excluir o conteúdo, impedir que o mesmo material seja novamente carregado e disponibilizado aos demais usuários.

Neste cenário, passa-se a analisar os modelos de responsabilização dos provedores de aplicações de internet mencionados e o julgamento da matéria pelo Supremo Tribunal Federal. Ao final, ver-se-á que, admitida a inconstitucionalidade do artigo 19 do Marco Civil da Internet, a adoção de um modelo geral, amparado no sistema de *notice and take down*, pode proporcionar maior resguardo aos direitos e garantias constitucionais em evidência.

2. O MODELO DE NOTICE AND TAKE DOWN

Antes de adentrar o enfrentamento da questão da responsabilização do provedor de aplicações de internet por conteúdo elaborado por terceiros no Brasil, vale refletir sobre o modelo *notice and take down*, voltado para a responsabilização dos provedores de hospedagem atualmente vigente em diversos países, de modo a, posteriormente, compará-lo com o modelo nacional e enfrentar a discussão travada sobre a (in)constitucionalidade do art. 19 do Marco Civil da Internet.

Na União Europeia, no ano de 2000, foi publicada a Diretiva 2000/31/CE relativa a “*certos aspectos legais dos serviços da sociedade de informação, em especial do comércio eletrônico, no mercado interno*”.¹¹ Tal Diretiva, elaborada pelo Parlamento

fraterna, pluralista e sem preconceitos, fundada na harmonia social e comprometida, na ordem interna e internacional, com a solução pacífica das controvérsias, promulgamos, sob a proteção de Deus, a seguinte CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL”.

11. UNIÃO EUROPEIA. *Diretiva 2000/31/CE do Parlamento Europeu e do Conselho*, relativa a certos aspectos legais dos serviços da sociedade de informação, em especial do comércio eletrônico, no mercado interno («Directiva sobre o comércio electrónico»), 08 jun. 2000. Disponível em: <<https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex%3A32000L0031>>, acesso em: 01

Europeu, cuidou de estabelecer objetivos, no âmbito comunitário, para a utilização da internet como meio de exercício de atividade econômica, constituindo a base legislativa do sistema de *notice and take down* na União Europeia.¹²

A Diretiva europeia baseou-se no modelo americano, especificamente nos atos denominados *Communications Decency Act*, de 08 de fevereiro de 1996, e *Digital Millennium Copyright Act*, de 12 de outubro de 1998.¹³ Segundo tal modelo, a responsabilidade do provedor de aplicações de internet pela veiculação, por terceiros, de conteúdo ilícito será excluída quando estiverem presentes três condições, sendo elas (i) a ignorância da atividade ilícita, (ii) a colaboração na coibição do ato, no momento em que ocorrer o conhecimento e (iii) a ausência de um benefício econômico diretamente atrelado à ilicitude.

É importante destacar que, nos Estados Unidos, o *Communications Decency Act* e o *Digital Millennium Copyright Act* dizem respeito apenas ao direito de autor, de modo que o modelo de *notice and take down* possui aplicação apenas para a veiculação de conteúdo que viola direitos autorais. Por outro lado, a Diretiva da União Europeia inova ao estabelecer regra abrangente, aplicável aos conteúdos ilícitos de qualquer natureza veiculados pelo que a doutrina conceitua como *host providers* (conceito abrangido na legislação brasileira pelo termo provedor de aplicações de internet).¹⁴

Em relação à atividade de armazenagem em servidor, a Diretiva europeia traz uma vedação à responsabilização dos provedores prestadores desse tipo de serviço em razão de conteúdo ilícito postado por terceiros e as hipóteses em que, excepcionalmente, restará configurada a responsabilidade civil.¹⁵

jan. 2025.

12. ANGELOPOULOS, Christina; SMET, Stijn. Notice-and-Fair-Balance: How to reach a compromise between fundamental rights in european intermediary liability. *Journal of media law*, vol. 8, 2016, p. 3. Disponível em: <<http://dx.doi.org/10.2139/ssrn.2944917>>, acesso em: 01 jan. 2025.

13. MANTELERO, Alessandro. *Diritto dell'informatica*. Milano: UTET, 2014, p. 792/793.

14. IPPOLITO, Fulvio Sarzana Di S. *I contratti di internet e del commercio elettronico*, Milano: A. Giuffrè Editore, 2001, p. 70; LEONARDI, Marcel. *Responsabilidade civil dos provedores dos serviços de internet*. São Paulo: Juarez de Oliveira, 2005, p. 25, e-book.

15. O artigo 14 da Diretiva 2000/31/CE dispõe o seguinte: “Artigo 14. Armazenagem em servidor. 1. Em caso de prestação de um serviço da sociedade da informação que consista no armazenamento

Como se vê, o provedor de hospedagem será responsabilizado apenas quando tiver efetivo conhecimento da ilicitude do fato ou da informação e, em relação a eventual ação de ressarcimento por danos, apenas quando tenha conhecimento de fatos ou circunstâncias que tornem manifesta a ilicitude. Além disso, é imprescindível, para a caracterização da responsabilidade, a ausência de atuação imediata para a remoção do conteúdo.¹⁶

Concomitantemente, o Considerando nº 42 da Diretiva 2000/31/CE¹⁷ prevê, expressamente, que as isenções trazidas pela legislação se aplicam ao exercício da atividade dos provedores que seja estritamente técnica, automática e de natureza passiva. O provedor de hospedagem, por consequência, será isento da responsabilização apenas quando não possuir conhecimento (ou controle) da informação transmitida ou armazenada, agindo passivamente na sua veiculação.

Ressalta-se, ainda, que o art. 15 da Diretiva 2000/31/CE prevê, expressamente, a ausência de obrigação geral de vigilância pelo provedor de hospedagem. A ausência

de informações prestadas por um destinatário do serviço, os Estados-Membros velarão por que a responsabilidade do prestador do serviço não possa ser invocada no que respeita à informação armazenada a pedido de um destinatário do serviço, desde que: a) O prestador não tenha conhecimento efetivo da atividade ou informação ilegal e, no que se refere a uma ação de indenização por perdas e danos, não tenha conhecimento de factos ou de circunstâncias que evidenciam a atividade ou informação ilegal, ou b) O prestador, a partir do momento em que tenha conhecimento da ilicitude, atue com diligência no sentido de retirar ou impossibilitar o acesso às informações. 2. O nº 1 não é aplicável nos casos em que o destinatário do serviço atue sob autoridade ou controlo do prestador. 3. O disposto no presente artigo não afeta a faculdade de um tribunal ou autoridade administrativa, de acordo com os sistemas legais dos Estados-Membros, exigir do prestador que previna ou ponha termo a uma infracção, nem afeta a faculdade de os Estados-Membros estabelecerem disposições para a remoção ou impossibilitação do acesso à informação”.

16. ANGELOPOULOS, Christina; SMET, *op. cit.*, p. 3.

17. Diretiva 2000/31/CE Considerando nº 42: “As isenções da responsabilidade estabelecidas na presente directiva abrangem exclusivamente os casos em que a actividade da sociedade da informação exercida pelo prestador de serviços se limita ao processo técnico de exploração e abertura do acesso a uma rede de comunicação na qual as informações prestadas por terceiros são transmitidas ou temporariamente armazenadas com o propósito exclusivo de tornar a transmissão mais eficaz. Tal actividade é puramente técnica, automática e de natureza passiva, o que implica que o prestador de serviços da sociedade da informação não tem conhecimento da informação transmitida ou armazenada, nem o controlo desta”.

de dever de vigilância, por sua vez, se aplicará aos provedores que exerçam atividade meramente passiva, sem qualquer interferência no conteúdo, conforme esclarecido pelo Considerando nº 42, sendo certo que agindo o provedor em tempo hábil para a retirada do ar de conteúdo ilícito, logo que tomado conhecimento, não restará configurada a responsabilidade civil.¹⁸

No âmbito da jurisprudência comunitária, dois são os casos de destaque para a definição da responsabilidade civil do provedor de hospedagem após a publicação da Diretiva 2000/31/CE. No julgamento dos casos *Google France, Google Inc. v. Louis Vuitton Malletier*¹⁹ (Sentença C-236/08; C-238/08 de 23 de março de 2010) e *L’Oreal SA v. eBay International AG*²⁰ (Sentença C-324/09 de julho de 2011), as cortes europeias consolidaram o entendimento previsto na Diretiva, dando-lhe eficácia no âmbito jurisprudencial.

O primeiro caso diz respeito à responsabilidade da plataforma Google, em relação ao software *Google Ads*, um serviço de publicidade mediante pagamento, por meio do qual foram veiculados, sem autorização, conteúdos protegidos pelo direito de marcas. A *Grand Chamber* da *European Court of Justice*, tendo como embasamento o Considerando nº 42 da Diretiva 2000/31/CE, entendeu que a responsabilidade civil se aplicaria ao prestador de serviço de hospedagem apenas quando este tenha desenvolvido um papel ativo na veiculação do conteúdo, de acordo com o qual adquira conhecimento ou controle dos dados memorizados, o que não teria ocorrido no caso concreto.

Trata-se de julgado que consolidou, na prática, o disposto na Diretiva 2000/31/CE, prevendo, ainda, que a responsabilidade incidiria também no caso em que, tendo desenvolvido papel passivo, ao tomar conhecimento da ilicitude, o

18. MANTELERO, Alessandro. *Op. cit.*, p. 798/799.

19. UNIÃO EUROPEIA. Acórdão do Tribunal de Justiça (Grande Secção) de 23 de março de 2010. *Google France SARL and Google Inc. v Louis Vuitton Malletier SA*, C-236/08, ECLI:EU:C:2010:159. Disponível em: <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62008CJ0236>>, acesso em 02 jan. 2025.

20. UNIÃO EUROPEIA. Acórdão do Tribunal de Justiça (Grande Secção) de 12 de julho de 2011. *L’Oréal SA and Others v eBay International AG and Others*, C-324/09. ECLI:EU:C:2011:474. Disponível em: <<https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A62009CJ0324>>, acesso em 02 jan. 2025.

provedor não tenha agido diligentemente para sua remoção, nos exatos termos do previsto no artigo 14 da Diretiva 2000/31/CE.

Posteriormente, no caso *L’Oreal SA v. eBay International AG*, em que a plataforma *eBay*, tratando de seu mercado eletrônico, adicionou filtros de pesquisa que permitiam a identificação de preferência e sugestão de produtos para os compradores do canal, concorrendo para a venda de produtos defeituosos, foi considerada responsável solidária. A Corte aprofundou no tema da responsabilidade civil do provedor de hospedagem, introduzindo dois relevantes conceitos para a interpretação do artigo 14 da Diretiva 2000/31/CE.

O primeiro é referente ao estado de “passividade” do provedor de hospedagem, tendo sido fixado o entendimento de que o provedor deixa de exercer seu serviço de maneira passiva naqueles casos em que tenha prestado uma assistência consistente na otimização da prestação e na promoção de ofertas.

O segundo identificador proposto na sentença se refere ao momento em que o provedor de hospedagem é considerado ciente da informação ilícita veiculada. A Corte definiu que existem ao menos duas hipóteses para a configuração da ciência inequívoca, sendo elas a execução de um controle de iniciativa do provedor de hospedagem, em que seria possível a constatação do ilícito, ou a notificação acerca da existência de uma atividade ou uma informação ilícita.

Portanto, a partir da Diretiva 2000/31/CE e sua posterior aplicação pela *European Court of Justice*, o sistema de *notice and take down* se consolidou na União Europeia, tendo, posteriormente, surgido em outros atos²¹ e sido incorporado pela legislação dos países-membros.²²

21. No artigo 17 da *General Data Protection Regulation*, do ano de 2018, há adoção expressa do modelo de *notice and take down* para permitir que os usuários pleiteiem a exclusão de conteúdo por eles próprios publicados, sob o a perspectiva do direito ao esquecimento. O *caput* do dito dispositivo legal prevê o seguinte: “O titular tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada, e este tem a obrigação de apagar os dados pessoais, sem demora injustificada, quando se aplique um dos seguintes motivos: [...]” (UNIÃO EUROPEIA. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho. Regulamento Geral sobre a Proteção de Dados*, 27 abr. 2016. Disponível em: <<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>>, acesso em: 09 fev. 2025).

22. Os atos correspondentes à incorporação da Diretiva 2000/31/CE podem ser acessados no link a

Neste cenário, merece destaque a Lei alemã, cujo escopo é a melhoria da aplicação da lei nas redes sociais, chamada *Netzwerkdurchsetzungsgesetz - NetzDG*, que passou a vigorar em 1º de outubro de 2017. O sistema de *notice and take down* já era utilizado no país desde 2001, à luz da Diretiva 2000/31/CE, porém, com o rápido avanço e o aumento do número de usuários das plataformas digitais, foi elaborada a normativa direcionada especialmente às redes sociais, que merece destaque por trazer disposições inovadoras e mais rigorosas para as plataformas digitais.²³

Na forma em que inicialmente promulgado, o NetzDG se aplicava especificamente às redes sociais, entendidas como plataformas digitais, com fins lucrativos, que permitiam o compartilhamento de conteúdo com os demais usuários e que possuíam dois milhões ou mais de usuários inscritos na Alemanha.²⁴ A legislação determinava que as plataformas de redes sociais teriam vinte e quatro horas para excluir conteúdo manifestamente ilícito, sob pena de aplicação de multa de até cinquenta milhões de euros.

Conquanto a aplicação do sistema de *notice and take down* não fosse uma novidade, a legislação foi pioneira na aplicação de multa elevada e na especificação de prazos para remoção. Caso houvesse dúvida acerca da “manifesta” ilegalidade, o processo de remoção poderia estender-se em até sete dias.

Em relatório do período entre janeiro e junho de 2023, a plataforma Youtube informou ter recebido 193.131 denúncias de conteúdo ilícito, sendo que, desse total, foram removidas 30.870 postagens.²⁵ A elaboração de relatórios contendo tais informações também era uma obrigação prevista na legislação, visando a um tratamento mais transparente.

seguir: <Directive - 2000https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX:32000L003131 - EN - e-commerce directive - EUR-Lex>, acesso em: 01 jan. 2025.

23. ZURTH, Patrick. The German NetzDG as Role Model or Cautionary Tale? Implications for the Debate on Social Media Liability. *Fordham Intellectual Property, Media and Entertainment Law Journal*. 31 Fordham Intell. Prop. Media & Ent. L.J. 1084 (2021). Disponível em: <https://ir.law-net.fordham.edu/iplj/vol31/iss4/4>, acesso em: 09 fev. 2025.

24. BREGA, Gabriel. A regulação de conteúdo nas redes sociais: uma breve análise comparativa entre o NetzDG e a solução brasileira. *Revista direito gv*, v. 19, e2305, São Paulo, 2023, p. 13.

25. O relatório foi disponibilizado pela plataforma no link a seguir: <https://transparencyreport.google.com/netzdg/youtube?hl=pt_BR>, acesso em: 04 jan. 2025.

Apesar de pioneiras, as especificações previstas no NetzDG não se encontram mais vigentes em razão da entrada em vigor do *Digital Services Act*. Trata-se de uma norma da União Europeia (*Regulation 2022/2065*) relativa a um mercado único para os serviços digitais e que alterou a Diretiva 2000/31/CE.²⁶

O *Digital Services Act*, enquanto uma ferramenta de atualização da 2000/31/CE, mantém o modelo de *notice and take down* e traz maiores informações sobre a moderação de conteúdo pelos provedores de hospedagem.²⁷ Em relação ao NetzDG, é considerado menos rigoroso, já que não especifica o prazo de remoção do conteúdo ilícito. Por outro lado, tem maior abrangência prática, já que se aplica a toda e qualquer plataforma digital, não havendo um número mínimo de usuários inscritos.

Fica claro, portanto, que o modelo de *notice and take down* prevalece no âmbito da União Europeia, tendo perpassado por atualizações ao longo dos anos e sendo adotado pelos países comunitários, em consonância com legislações próprias.

3. O MODELO DE NOTICE AND STAY DOWN

Apesar do bom funcionamento do sistema de *notice and take down* ao longo dos anos, que resultou em sua aplicação até o presente momento, na União Europeia e no caso de direito de autor nos Estados Unidos, o sistema não está isento de críticas. Uma das mais relevantes críticas diz respeito ao direito de autor.

Segundo os titulares do direito de autor, o sistema proposto é caro, não seria apto a combater a pirataria *online* em massa e ainda fortaleceria a concorrência desleal.²⁸ Neste cenário, em março de 2019, foi aprovada, na União Europeia, a Diretiva 2019/790, que dispõe sobre os direitos autorais no Mercado Único Digital.

26. UNIÃO EUROPEIA. *Regulamento (UE) 2022/2065 do Parlamento Europeu e do Conselho*, relativo a um mercado único para os serviços digitais e que altera a Diretiva 2000/31/CE, 19 out. 2022. Disponível em: <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065>>, acesso em: 01 jan. 2025.

27. BUITEN, Miriam. The digital services act from intermediary liability to platform regulation. 12 *Journal of intellectual property, information technology and electronic commerce law*, p. 363, 2021.

28. CASTRO, Carla Frade de Paula. Responsabilidade civil dos provedores de aplicações de internet por infrações de terceiros a direitos autorais. *Revista de informação legislativa*, v. 60, n. 237, p. 141-171, jan./mar. 2023, p. 152.

No que interessa, no campo da responsabilidade civil concernente à proteção dos direitos autorais, a Diretiva de 2019 inaugura, na União Europeia, o chamado modelo de *notice and stay down*.

A partir das disposições do artigo 17 da referida Diretiva,²⁹ provedores que disponibilizem conteúdos gerados por terceiros e protegidos pelo direito de autor deverão realizar um ato de comunicação ao público, para o qual é necessária a obtenção de autorização junto ao titular do direito. Caso não sejam tomadas as medidas sugeridas na Diretiva, os provedores poderão responder solidariamente pela infração,

29. “Os Estados-Membros devem prever que os prestadores de serviços de partilha de conteúdos em linha realizam um ato de comunicação ao público ou de colocação à disponibilização do público para efeitos da presente diretiva quando oferecem ao público o acesso a obras ou outro material protegido por direitos de autor carregados pelos seus utilizadores. Os prestadores de serviços de partilha de conteúdos em linha devem, por conseguinte, obter uma autorização dos titulares de direitos a que se refere o artigo 3º, n. 1 e 2, da Diretiva 2001/29/CE, por exemplo, através da celebração de um acordo de concessão de licenças, a fim de comunicar ao público ou de colocar à disposição do público obras ou outro material protegido. [...] 3. Quando os prestadores de serviços de partilha de conteúdos em linha realizam atos de comunicação ao público ou de colocação à disposição do público nas condições estabelecidas na presente diretiva, a limitação da responsabilidade prevista no artigo 14º, n.º 1, da Diretiva 2000/31/CE não se aplica às situações abrangidas pelo presente artigo. O disposto no primeiro parágrafo do presente número, não prejudica a possível aplicação do artigo 14º, n.º 1, da Diretiva 2000/31/CE a esses prestadores de serviços para fins não abrangidos pelo âmbito de aplicação da presente diretiva. 4. Caso não seja concedida nenhuma autorização, os prestadores de serviços de partilha de conteúdos em linha são responsáveis por atos não autorizados de comunicação ao público, incluindo a colocação à disposição do público, de obras protegidas por direitos de autor e de outro material protegido, salvo se os prestadores de serviços demonstrarem que: a) Envidaram todos os esforços para obter uma autorização; e b) Efetuaram, de acordo com elevados padrões de diligência profissional do setor, os melhores esforços para assegurar a indisponibilidade de determinadas obras e outro material protegido relativamente às quais os titulares de direitos forneceram aos prestadores de serviços as informações pertinentes e necessárias e, em todo o caso; c) Agiram com diligência, após resseção de um aviso suficientemente fundamentado pelos titulares dos direitos, no sentido de bloquear o acesso às obras ou outro material protegido objeto de notificação nos seus sítios Internet, ou de os retirar desses sítios e envidaram os melhores esforços para impedir o seu futuro carregamento, nos termos da alínea b).” (UNIÃO EUROPEIA. *Diretiva 2019/790 do Parlamento Europeu e do Conselho*, relativa aos direitos de autor e direitos conexos no mercado único digital e que altera as Diretivas 96/9/CE e 2001/29/CE, 17 abr. 2019. Disponível em: <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019L0790>>, acesso em: 01 jan. 2025).

juntamente com o usuário que fez o *upload*.³⁰

Para afastar a responsabilização das plataformas, devem ser cumpridas uma série de obrigações, que demonstram uma atuação diligente da plataforma para coibir a infração ao direito de autor, conforme item 4 do artigo 16. Entre os requisitos para se afastar a responsabilidade objetiva dos provedores, encontra-se a obrigação de empregar os melhores esforços para impedir o *upload* futuro de obras que foram retiradas após uma notificação dos titulares, o que constitui o chamado modelo de *notice and stay down*.³¹

É importante ressaltar que o apelo dos titulares de direito de autor não era novidade quando da elaboração da Diretiva, tendo sido, inclusive, objeto de relevantes críticas em relação ao Direito norte-americano, que prevê apenas o sistema de *notice and take down* nessa seara. Portanto, ao longo dos anos, o modelo de *notice and stay down* foi sendo construído no bojo da própria jurisprudência da União Europeia.

Caso relevante também sob essa perspectiva é o da *L'Oreal SA v. eBay International AG*, já mencionado. Sobre o modelo do *notice and stay down*, o julgado prevê que as medidas cautelares do artigo 11 da Diretiva 2000/31/CE servem não apenas para atos que contribuam para pôr fim à divulgação de conteúdo ilícito, mas, também, para evitar novas infrações. No entanto, a Corte europeia previu que a prevenção de novas infrações não pode ser obtida por meio de um monitoramento ativo de todos os dados de cada um dos usuários de um intermediário *on-line*.

Destarte, de acordo com a *European Court of Justice*, um provedor de hospedagem poderá ser obrigado a suspender o acesso do responsável por uma violação de direito de autor para evitar (i) outras violações desse tipo (ii) pelo mesmo infrator (iii) em relação às mesmas marcas ou direito autoral registrado.³² Em outras palavras,

30. KUCZERAWY, Aleksandra. From 'notice and take down' to 'notice and stay down': risks and safeguards for freedom of expression. In: Giancarlo Frosio (ed) *The Oxford handbook of intermediary liability online*, 2019. Disponível em: <<https://ssrn.com/abstract=3305153>>, acesso em: 04 jan. 2025.

31. CASTRO, Carla Frade de Paula. *Op. cit.*, p. 153; VALENTE, Mariana Giorgetti. *Direito autoral e plataformas de internet: um assunto em aberto*. InternetLab, 18 abr. 2019. Disponível em: <<https://internetlab.org.br/pt/especial/direito-autoral-e-plataformas-de-internet-um-assunto-em-aberto/>>, acesso em: 04 jan. 2025.

32. UNIÃO EUROPEIA. *Diretiva 2019/790 do Parlamento Europeu e do Conselho*, relativa aos

a solução encontrada pela Corte diz respeito à suspensão de acesso ao provedor por parte do perpetrador do ato ilícito.

Diante da natureza de Diretiva, que deve ser incorporada ao direito dos países membro, a seu próprio modo, o modelo de *notice and stay down* previsto na Diretiva 2019/790 já vem sendo adotado pelos países comunitários.

Enquanto, na Europa, o modelo de *notice and take down* passou por evolução e desdobramentos que resultaram na criação do modelo de *notice and stay down* para os casos do direito de autor, no Brasil, ainda se discute a aplicação do modelo mais antigo, conforme será visto a seguir.

4. A RESPONSABILIDADE CIVIL DOS PROVEDORES DE APLICAÇÕES NO MARCO CIVIL DA INTERNET

No Brasil, o artigo 19 do Marco Civil da Internet condicionou a responsabilização do provedor, pela veiculação de conteúdo ilícito gerado por terceiros, ao desatendimento de uma ordem judicial específica de torná-lo indisponível. Isto significa que os provedores de aplicações de internet serão responsabilizados pela veiculação de conteúdo ilícito gerado por terceiros apenas quando, em face de ordem judicial específica, se abstiverem de agir, deixando de remover o conteúdo.

A limitação da responsabilidade civil dos provedores de hospedagem aos casos em que haja determinação judicial no sentido de remoção do conteúdo, é justificada pelo “*intuito de assegurar a liberdade de expressão e impedir a censura*”, conforme disposto, expressamente, no Texto legal. Ao assim determinar, o legislador cria a possibilidade da veiculação dos mais diversos conteúdos ilícitos, tais como a venda de produtos ilícitos e a reprodução de imagens degradantes, como, por exemplo, de *bullying*, sem que o provedor de hospedagem tenha o dever de agir para assegurar o direito violado de terceiro até que se obtenha uma determinação judicial.

O modelo proposto pelo artigo 19 do Marco Civil da Internet se aproxima do modelo adotado no Chile, para os casos de direito de autor, em que o provedor de

direitos de autor e direitos conexos no mercado único digital e que altera as Diretivas 96/9/CE e 2001/29/CE, 17 abr. 2019. Disponível em: <<https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX:32019L0790>>, acesso em: 01 jan. 2025.

aplicações, quando notificado, apenas possui a obrigação de notificar a parte que fez o *upload* do conteúdo ilegal (modelo conhecido como *notice and notice*), ficando reservada, ao Poder Judiciário, a possibilidade de ordenar a exclusão do conteúdo.³³

Como exceção à regra geral, em seu artigo 21,³⁴ o Diploma legal prevê que o conteúdo disponibilizado pelos provedores de aplicações de internet e gerado por terceiros que contenham imagens, vídeos ou outros materiais com cenas de nudez ou atos sexuais de caráter privado, implicará em responsabilidade subsidiária do provedor se, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo.

Percebe-se que a responsabilidade civil dos provedores de internet pelos atos praticados por terceiros está limitada, regra geral, à abstenção e à omissão do provedor, após determinação judicial de remoção do conteúdo, com a exceção dos casos que versem sobre imagens de nudez ou atos sexuais, em que a legislação prevê que a simples notificação do ofendido basta para atribuir responsabilidade subsidiária ao provedor que se abster de agir.

Contudo, o disposto no art. 19 do Marco Civil da Internet foi submetido ao crivo do Supremo Tribunal Federal. A Corte Suprema definiu o Tema de Repercussão Geral nº 987, que discutiu a constitucionalidade do dispositivo legal que determina a necessidade prévia e específica de ordem judicial de exclusão de conteúdo para a responsabilização civil de provedor de internet, website e gestores de aplicativos de redes sociais por danos decorrentes dos atos ilícitos praticados por terceiros. Como mencionado, o julgamento ocorre em conjunto com o Tema de Repercussão Geral nº 533.

33. SILVA, Alberto Jacob Cerda. Chile. In: Dumortier, Jos; Gryffroy, Pieter; Roex, Ruben; Van Der Syte, Yung Shin (eds.), *IEL privacy and technology law*. Kluwer law international bv, Netherlands, p. 131, 2020.

34. “Art. 21. O provedor de aplicações de internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo.”

Os pontos principais da controvérsia referentes ao aludido art. 19 envolveram o seguinte: (i) o dispositivo legal violaria o direito constitucional à imagem; (ii) haveria afronta ao princípio do acesso à justiça, em sua forma substancial; (iii) haveria violação ao princípio de vedação de retrocesso (em relação ao grau de proteção que já era concedido aos direitos fundamentais pela jurisprudência brasileira); (iv) haveria violação à hierarquia de valores constitucionais; e (v) a obrigação de se acionar o Poder Judiciário seria medida desproporcional, já que exige imenso esforço da vítima.³⁵

O julgamento de (in)constitucionalidade do artigo 19, que estabelece o modelo para responsabilização dos provedores de aplicações de internet por conteúdo gerado por terceiros no Brasil, decorre de ampla discussão doutrinária e jurisprudencial travada no país. Além disso, teve, como pano de fundo, o questionamento acerca da aplicabilidade do modelo de *notice and take down*. Sobre o tema, prezando pela adoção do sistema de *notice and take down*, Anderson Schreiber afirma que, ao condicionar a responsabilidade civil dos provedores ao descumprimento de ordem judicial específica, “o referido art. 19 promove um espantoso engessamento da tutela dos direitos do usuário da internet, não raro, direitos fundamentais expressamente protegidos pela Constituição da República como a honra, a imagem e a privacidade”.³⁶ Segundo defende o autor, estaríamos diante de “verdadeira bolha de irresponsabilidade”, já que os terceiros que disponibilizam conteúdo ilícito são, na maior parte das vezes, anônimos, sendo que, não raro, a sua identidade e localização apenas pode ser conhecida pelos próprios provedores de aplicações de internet.

Destaca-se, ainda, o posicionamento de Barreto Júnior e Leite,³⁷ ao afirmarem que, “em se tratando da sociedade da informação, com a instantaneidade das notícias,

35. SCHREIBER, Anderson; RIBAS, Felipe; MANSUR, Rafael. *Deepfakes: regulação e responsabilidade civil*. In: TEPEDINO, Gustavo; SILVA, Rodrigo da Guia (Coord.). *O direito civil na era da inteligência artificial*. São Paulo: Thomson Reuters Brasil, 2020. p. 623/624.

36. SCHREIBER, Anderson. Marco civil da internet: avanço ou retrocesso? A responsabilidade civil por dano derivado do conteúdo gerado por terceiro. In: LUCCA, Newton de; SIMÃO FILHO; Adalberto; LIMA, Cíntia Rosa Pereira de (Coords). *Direito & internet III - Tomo II: marco civil da internet* (Lei nº 12.965/2014). São Paulo: Quartier Latin, 2015, p. 304.

37. BARRETO JÚNIOR, I. F.; FERREIRA LEITE, B. S. Responsabilidade civil dos provedores de aplicações por ato de terceiro na lei 12.965/14 (marco civil da internet). *Revista brasileira de estudos políticos*, v. 115, 27 nov. 2017, p. 432.

mais parece que levar o caso ao Judiciário causou um grande retrocesso frente à necessidade de uma resposta imediata à ofensa". Portanto, para aqueles que criticam a disposição trazida no Marco Civil da Internet, a exclusão de responsabilidade dos provedores de aplicações de internet até que haja uma abstenção em face de uma determinação judicial acaba por dificultar e engessar a defesa do ofendido, criando um sistema desequilibrado.³⁸

Nessa linha, Leonardi³⁹ defendia, antes da vigência do Marco Civil da Internet, que o provedor de hospedagem poderia ser responsabilizado quando *"deixar de bloquear o acesso à informação ilegal disponibilizada por um usuário, ou quando não fizer em tempo hábil, desde que tenha sido previamente informado a esse respeito e desde que não haja dúvidas sobre a ilicitude da conduta"*. À época, segundo entendimento de tal autor, os provedores de hospedagem não seriam responsabilizados apenas diante da existência de controvérsia em relação à ilicitude.⁴⁰

Recentemente, após a vigência do artigo 19 do Marco Civil da Internet e diante da discussão instaurada perante o Supremo Tribunal Federal, o autor passou a defender que *"o artigo 19 previne a censura privada indiscriminada, baseada em alegações unilaterais. Rejeitar essa salvaguarda significaria retroceder a um cenário de insegurança jurídica e censura que já superamos"*.⁴¹

No mesmo sentido do posicionamento adotado mais recentemente por Leonardi,

38. MIRAGEM, Bruno. *Direito civil. Responsabilidade civil*. São Paulo: Saraiva, 2015, p. 807; GODOY, Claudio Luiz Bueno de. Uma análise crítica da responsabilidade civil dos provedores na Lei n. 12.965/14 (Marco Civil da Internet). In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). *Direito & internet III – Tomo II: marco civil da internet (Lei n. 12.965/2014)*. São Paulo: Quartier Latin, 2015, p. 307-320; VAINZOF, Rony. Da responsabilidade por danos decorrentes de conteúdos gerados por terceiros. In MASSO, F. del; ABRUSIO, J.; FLORENCIO FILHO, Marco A. (Coord.). *Marco civil da internet: Lei 12.965/2014*. São Paulo: RT, 2014. p.177-205.

39. LEONARDI, Marcel. *Responsabilidade civil dos provedores dos serviços de internet*. São Paulo: Juarez de Oliveira, 2005, e-book, p. 107.

40. LEONARDI, Marcel. Op. cit., p. 108.

41. LEONARDI, Marcel. *Cem motivos para o STF preservar o artigo 19*. Estadão. Disponível em <<https://www.estadao.com.br/opiniaio/espaco-aberto/cem-motivos-para-o-stf-preservar-o-artigo-19/?srsltid=AfmBOoqHMTbvRaCZxUNUCz15jv2S69lUrpy0KT6AqzpeWiacINgjoHe1>>, acesso em 03 jan. 2025.

Teffé e Moraes⁴² explicam que: “*ao se colocar nas mãos do Judiciário a apreciação do conteúdo, garante-se uma maior segurança para os negócios desenvolvidos na internet, bem como a construção de limites com um maior grau de legitimidade para a expressão na rede*”. Do mesmo modo, Stoco⁴³ defendia que quando o provedor de internet age como mero fornecedor de meios físicos, “*não pode ser responsabilizado por eventuais excessos e ofensas à moral, à intimidade e à honra de outros*”.

Essencialmente, a disposição prevista no Marco Civil da Internet tem, como justificativa principal, a proteção da liberdade de expressão. Segundo Souza⁴⁴, “*o desenho do regime de responsabilidade civil por ato de terceiros no Marco Civil da Internet visa a assegurar que a liberdade de expressão não sofra restrições indevidas*”, sendo este o fundamento principal que justificou a elaboração de tal dispositivo legal, de modo que consta, expressamente, o alcance de tal objeto no texto legal.

Fato é, neste cenário, que a discussão doutrinária também chegou ao Superior Tribunal de Justiça. Anteriormente ao Marco Civil da Internet, a Corte Superior havia fixado o entendimento de que os provedores não respondiam objetivamente pelo conteúdo publicado por terceiros, porém, deveriam agir, diligentemente, sempre que tivessem conhecimento acerca de conteúdo ilícito por eles veiculados, para removê-los imediatamente.⁴⁵ Em outras palavras, o Superior Tribunal de Justiça aplicava o

42. TEFFÉ, Chiara Spadaccini de; MORAES, Maria Celina Bodin. Redes sociais virtuais: privacidade e responsabilidade civil. Análise a partir do marco civil da internet. *Pensar - Revista de ciências jurídicas*, 22(1), 108–46. p. 132.

43. STOCO, Rui. *Tratado de responsabilidade civil*. 6. ed. São Paulo: RT, 2004. p. 901.

44. SOUZA, Carlos Affonso Pereira de. As cinco faces de proteção à liberdade de expressão no marco civil da internet. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coord.). *Direito & internet III: marco civil da internet. Tomo II*. São Paulo: Quartier Latin, 2015, p. 397.

45. No julgamento do Recurso Especial nº 1.342.640, a Ministra Nancy Andrighi sintetizou o posicionamento do STJ, fixando o entendimento de que: (i) não respondem objetivamente pela inserção no site, por terceiros, de informações ilegais; (ii) não podem ser obrigados a exercer um controle prévio do conteúdo das informações postadas no site por seus usuários; (iii) devem, assim que tiverem conhecimento inequívoco da existência de dados ilegais no site, removê-los imediatamente, sob pena de responderem pelos danos respectivos; (iv) devem manter um sistema minimamente eficaz de identificação de seus usuários, cuja efetividade será avaliada caso a caso” (STJ, 3ª T., REsp. 1.342.640 –SP, Rel. Min. Nancy Andrighi, julg. 07.02.2017, DJe 14.02.2017). No mesmo sentido: STJ, 3ª T., REsp. 1.641.155-SP, Rel. Min. Nancy Andrighi,

sistema de *notice and take down*.

Após a vigência do Marco Civil da Internet e, por conseguinte, da disposição do artigo 19 do Texto legal, o Superior Tribunal de Justiça passou a seguir o disposto na referida Lei, alterando o seu posicionamento.⁴⁶

O modelo adotado no Brasil gerou grande polêmica sobre a adequabilidade da obrigação de provocação do Poder Judiciário para a obtenção de uma ordem de remoção de conteúdo, com amplo debate, na doutrina e na jurisprudência pátria. Diante desse cenário, em 28 de novembro de 2024, o Supremo Tribunal Federal retomou o julgamento do Tema 987, em conjunto com o Tema 533.

5. O JULGAMENTO DA MATÉRIA PELO SUPREMO TRIBUNAL FEDERAL

Como visto, no Tema 987 da Suprema Corte, debateu-se a constitucionalidade do art. 19 da Lei n. 12.965/2014. No acórdão em que foi reconhecida a repercussão geral do tema, consignou-se:

Insta definir aqui se, à luz dos princípios constitucionais e da Lei nº 12.965/2014, a empresa provedora de aplicações de internet possui os deveres (i) de fiscalizar o conteúdo publicado nos seus domínios eletrônicos, (ii) de retirar do ar informações reputadas como ofensivas mediante simples notificação extrajudicial e (iii) de se responsabilizar legalmente pela veiculação do aludido conteúdo antes da análise pelo Poder Judiciário.⁴⁷

julg. 13.06.2017, DJe 22.06.2017. STJ, 3ª T., REsp. 1.193.764 –SP, Rel. Min. Nancy Andrighi, julg. 14.12.2010, DJe 08.08.2011; STJ, 4ª T., REsp. 1.501.187 –RJ, Rel. Min. Marco Buzzi, julg. 16.12.2014, DJe 03.03.2015; STJ, 4ª T., AgRg no Recurso Especial 1.402.104 –RJ, Rel. Min. Raul Araújo, julg. 27.05.2014, DJe 18.06.2014.

46. TEFFÉ, Chiara; SOUZA, Carlos Affonso. Responsabilidade civil dos provedores na rede: análise da aplicação do marco civil da internet pelo Superior Tribunal de Justiça. *Revista IBERC*, Minas Gerais, v.1, n.1, p. 01-28, nov.-fev./2019, p. 21.

47. BRASIL. Supremo Tribunal Federal. RE 1037396. Recorrente: Facebook Serviços Online do Brasil Ltda., Recorrida: Lourdes Pavioto Correa. Relator: Ministro Dias Toffoli, 01 de março de 2018. Disponível em: <<https://jurisprudencia.stf.jus.br/pages/search/repercussao-geral9662/false>>, acesso em 13 jan. 2025.

O julgamento da matéria se deu em conjunto com o Tema 533 do Supremo Tribunal Federal (anterior ao Marco Civil da Internet), já mencionado.

No primeiro caso (Tema 987), o *leading case* foi o Recurso Extraordinário nº 1.037.396, de relatoria do Ministro Dias Toffoli, em que o Facebook Serviços Online do Brasil Ltda. foi condenado pela Segunda Turma do Colégio Recursal de Piracicaba, Estado de São Paulo, ao pagamento de indenização por deixar de excluir perfil falso, após notificação da requerente. Já no segundo caso (Tema 533), o *leading case* foi o Recurso Extraordinário nº 1.057.258, de relatoria do Ministro Luiz Fux, em que se discutiu o pedido de exclusão de uma comunidade ofensiva da extinta rede Orkut, assim como a hipótese de reparação civil diante da inércia do provedor.

Após a realização de audiências públicas e apresentação de manifestações por uma série de interessados na matéria, o julgamento conjunto dos Temas 987 e 533 foi iniciado no dia 27 de novembro de 2024. Em 26 de junho de 2025, o julgamento foi concluído, tendo prevalecido a tese de inconstitucionalidade (parcial) do artigo 19 do Marco Civil da Internet, por 8 votos a 3.

O primeiro voto proferido foi o do Ministro Dias Toffoli. O relator do Recurso Extraordinário n. 1.037.396 (Tema 987) propôs a declaração de inconstitucionalidade do artigo 19 do Marco Civil da Internet e a utilização do disposto no artigo 21 do mesmo Diploma legal, como regra geral (sistema de *notice and take down*).

A tese proposta pelo Ministro Dias Toffoli ainda prevê a responsabilidade objetiva dos provedores de aplicações de internet quando houver o impulsionamento de conteúdo, quando se tratar de perfil falso, quando se tratar de direito de autor e quando houver a prática de algum dos crimes elencados (crimes contra o Estado Democrático de Direito, crime de racismo e outros). Há também disposições gerais sobre deveres anexos dos provedores de aplicações e obrigação específica que obriga os provedores com sede no exterior e atuação no Brasil a constituírem representante no país.

Do ponto de vista da liberdade de expressão, o voto do Min. Dias Toffoli traz alguns pontos relevantes. O primeiro deles é a existência de “*indevida hierarquização entre a liberdade de expressão e outros direitos fundamentais*”. O Relator defende que o artigo 19 do Marco Civil da Internet propõe uma posição de preferência à liberdade de expressão em detrimento de outros direitos fundamentais, o que não encontra

ressonância no ordenamento jurídico-constitucional brasileiro.

Sobre o tema, Ingo Sarlet⁴⁸ afirma que ainda que a liberdade de expressão usufrua de uma posição preferencial, “*não há, ao fim e ao cabo, como deixar de considerar as exigências de proporcionalidade e de outros critérios aplicáveis a tais situações*”. Apoiando-se em tal conceituação, o Min. Dias Toffoli, em seu voto, conclui que não é razoável que o legislador permita, em nome da liberdade de expressão “*o assassinato de reputações, a incitação à violência e à discriminação, o discurso de ódio, etc., reduzindo ou flexibilizando, em tese e a priori, as salvaguardas constitucionais aos demais direitos fundamentais ou à própria democracia*”.

Em segundo lugar, sustenta que a declaração de inconstitucionalidade do artigo 19 do Marco Civil da Internet decorre da proteção insuficiente de direitos fundamentais à luz do postulado da proporcionalidade. Isto porque, ao condicionar a responsabilização dos provedores à sistemática da notificação judicial, o Marco Civil da Internet possibilita que os provedores de aplicações de internet se eximam “*de qualquer tipo de cautela para com o ambiente virtual e se desoneram, até mesmo, da análise das reclamações recebidas, seja de modo automatizado, seja por apreciação humana*”.

Nesse contexto, fere-se o binômio liberdade *versus* responsabilidade, ficando oprimidos nesse sistema outros direitos constitucionalmente garantidos, tais como a intimidade, a vida privada, a honra e a imagem das pessoas.

Por fim, o Ministro Dias Toffoli defende que o disposto no artigo 19 do Marco Civil da Internet feriria o princípio democrático e seus consectários, incluindo a própria liberdade de expressão. A esse respeito, conforme sustenta Paulo Bonavides,⁴⁹ a democracia constitui direito fundamental de quarta geração e, enquanto tal, merece proteção dos efeitos deletérios das *fake news*, amplamente utilizadas no contexto nacional.⁵⁰

48. SARLET, Ingo Wolfgang. Liberdade de expressão e biografias não autorizadas — notas sobre a ADI 4.815. Consultor Jurídico. 19 de junho de 2015. Disponível em: <<https://www.conjur.com.br/2015-jun-19/direitos-fundamentais-liberdade-expressao-biografias-nao-autorizadas>>, acesso em: 02 fev. 2024

49. BONAVIDES, Paulo. **Curso de direito constitucional**. 14ª ed. São Paulo: Malheiros, 2004, p. 569.

50. Segundo reportagem da Folha de S. Paulo, publicada em 16 de julho de 2024, “*o Brasil é o terceiro*

Em seguida, o Ministro Luiz Fux, ao proferir o seu voto, apesar de acompanhar o entendimento do Ministro Dias Toffoli em relação ao Recurso Extraordinário e à inconstitucionalidade do artigo 19 do Marco Civil da Internet, propôs a fixação de tese divergente. Segundo o voto do Ministro Luiz Fux, a disposição do artigo 19 não excluiria a possibilidade de responsabilização de provedores de aplicações de internet por veiculação de conteúdos gerados por terceiros, quando manifesta a ilicitude e, uma vez cientificados os provedores, deixassem de excluir imediatamente o conteúdo.

Seguindo a linha do voto do Ministro Dias Toffoli, sugeriu a obrigação de vigilância dos provedores para os casos de discurso de ódio, racismo, pedofilia, incitação à violência, apologia à abolição violenta do Estado Democrático de Direito e apologia ao Golpe de Estado. Também consignou, na tese sugerida, que é presumido o conhecimento de ilicitude nos casos em que há impulsionamento oneroso de postagens, hipótese em que a responsabilidade dos provedores seria objetiva.

O Ministro Luís Roberto Barroso, terceiro a votar, divergiu dos posicionamentos anteriores, para sugerir a tese de inconstitucionalidade parcial do artigo 19 do Marco Civil da Internet. Em seu voto, o Ministro Barroso propõe a ampliação do escopo das exceções previstas no Marco Civil da Internet, por meio da interpretação conforme à Constituição da expressão “*ressalvadas as disposições legais em contrário*” presente no dispositivo cuja inconstitucionalidade é discutida.⁵¹

Portanto, a tese proposta foi a de que a regra geral adotada passe a ser a aplicação do artigo 21 do Marco Civil de Internet (*notice and take down*), excluindo-se, de tal regra, os crimes contra a honra que, no seu entendimento, deverão ser retirados exclusivamente após decisão judicial. O Ministro também reforçou que a natureza da responsabilidade, inclusive nos casos de *notice and take down*, seria subjetiva e tal

maior mercado da Meta para WhatsApp – atrás somente de Índia e Indonésia – e é o país que mais manda áudios no mundo, quatro vezes mais do que qualquer outro”. Disponível em: <https://www1.folha.uol.com.br/tec/2024/07/idec-e-mpf-pedem-r-17-bilhao-do-whatsapp-na-justica-por-violacoes-a-lei-de-dados.shtml?utm_source=sharenativo&utm_medium=social&utm_campaign=sharenativo>, acesso em: 02 fev. 2025.

51. CARVALHO, Luísa. *Ponto a ponto*: entenda o voto de barroso sobre o artigo 19 do marco civil da internet. JOTA. Disponível em <<https://www.jota.info/stf/do-supremo/ponto-a-ponto-entenda-o-voto-de-barroso-sobre-o-artigo-19-do-marco-civil-da-internet>>, acesso em: 04 jan. 2025.

como os julgadores que o antecederam, propôs o dever de vigilância para os conteúdos objeto de impulsionamento pago.

Após o voto do Ministro Luís Roberto Barroso, houve um pedido de vista pelo Ministro André Mendonça, o que acarretou a suspensão do julgamento até 4 de junho de 2025. Em seu voto, o Ministro André Mendonça inaugurou posicionamento integralmente divergente, no sentido da constitucionalidade do artigo 19 do Marco Civil da Internet.

O voto divergente ampara-se na máxima de que a liberdade de expressão seria indispensável à defesa dos demais direitos constitucionais e, conseqüentemente, teria preferência. Segundo o entendimento do Ministro André Mendonça, a retirada do requisito do descumprimento de ordem judicial para fins de responsabilização dos provedores taria o risco de censura ilegítima da manifestação de ideias e opiniões por parte de empresa privada.

Além disso, o Ministro reforçou, em seu voto, que as decisões judiciais de remoção devem seguir o devido processo legal. Igualmente, consignou a importância da autorregulação das plataformas digitais, o que permite a exclusão de conteúdos que violem as respectivas políticas e desde que sejam seguidos protocolos mínimos de proteção ao usuário, tais como o acesso aos fundamentos da exclusão e o direito de recurso e resposta em tempo razoável.

Ao final, o Ministro André Mendonça, propôs a interpretação do art. 19 do Marco Civil da Internet em consonância com a Constituição brasileira para: (i) definir que os serviços de mensagem não se equiparam aos de mídia social; (ii) declarar inconstitucional a remoção ou suspensão de perfis nas redes sociais, exceto quando forem falsos ou tiverem como objeto a prática de atividade criminosa; (iii) declarar a responsabilidade das plataformas em identificar o usuário violador do direito de terceiro, nos termos dos arts. 15 e 22 do Marco Civil da Internet; (iv) determinar que a remoção de conteúdos por violação às políticas dos provedores garanta direitos ao usuário violador de compreender e contestar a decisão; (v) determinar que, excetuados os casos previstos em lei, os provedores não possam ser responsabilizados por conteúdo ilícito gerado por terceiros e (vi) determinar a necessidade de fundamentação específica das decisões judiciais que determinarem a remoção de conteúdo.

Os Ministros Edson Fachin e Nunes Marques, apesar de terem apresentado

fundamentação diversa, também votaram pela constitucionalidade do artigo 19 do Marco Civil da Internet. O primeiro destacou que embora seja necessária uma maior proteção dos direitos fundamentais, a solução não deveria comprometer o equilíbrio entre liberdade de expressão e responsabilidade, reiterando o risco de que a responsabilização das plataformas digitais, sem a intervenção do Poder Judiciário, poderá acarretar o controle indevido de discursos.

Já o Ministro Nunes Marques, último a votar, reassaltou a competência do Congresso Nacional para promover a discussão sobre o tema e reforçou o entendimento dos votos pela constitucionalidade do artigo 19 do Marco Civil da Internet, no sentido de que a liberdade de expressão, enquanto cláusula pétrea da Constituição Federal, deveria ser protegida. O Ministro admitiu a possibilidade de remoção de conteúdo sem ordem judicial apenas quando houvesse prova de fraude, como quando houvesse uso indevido da imagem, em proteção aos direitos fundamentais à intimidade e à honra.

Os Ministros Cristiano Zanin, Flávio Dino, Gilmar Mendes, Alexandre de Moraes e Carmem Lúcia, seguindo o posicionamento do Min. Luís Roberto Barroso, votaram pela inconstitucionalidade parcial do artigo 19 do Marco Civil da Internet, tese que prevaleceu no julgamento. Apesar de cada um deles ter fundamentado o respectivo voto de maneira diversa, ao final do julgamento, chegou-se a uma tese comum.

Com efeito, o Supremo Tribunal Federal declarou parcialmente inconstitucional o artigo 19 do Marco Civil da Internet, tendo fixado treze pontos sobre o tema:

- 1) o dispositivo legal é parcialmente inconstitucional, visto que a regra não confere proteção suficiente a bens jurídicos fundamentais relevantes;
- 2) enquanto não sobrevier legislação apropriada – reconhecendo a necessidade de renovação no âmbito legislativo – deverá haver a interpretação conforme dos artigos 19 do Marco Civil da Internet para que os provedores sejam responsabilizados civilmente, ressalvada a aplicação de disposição específicas da legislação eleitoral;
- 3) os provedores de aplicações de internet serão responsabilizados na forma do art. 21 do Marco Civil da Internet, ou seja, pelo modelo de

notice and take down, em casos em que o conteúdo veiculado corresponder a crime, com excessão dos crimes à honra, ou atos ilícitos. Além disso, quando houver sucessivas replicações de fato ofensivo já reconhecido por decisão judicial, deverão ser removidos conteúdos idênticos, inclusive por outros provedores – proposição que se assemelha ao *notice and stay down*;

- 4) haverá a presunção de responsabilidade dos provedores pela veiculação de conteúdo ilícito quando for o caso de anúncios ou impulsionamento pago e em casos em que houver uso de rede artificial de distribuição (*chatbot* ou robôs). Pode haver responsabilização mesmo sem notificação, salvo se o provedor agir de forma diligente e rápida;
- 5) deverá haver dever de cuidado em casos de circulação massiva de conteúdos ilícitos graves previstos em rol taxativo proposto pelo Supremo Tribunal Federal.
- 6) a aplicação do artigo 19 do Marco Civil da Internet permanece para provedores de e-mail plataformas de reunião fechadas e serviços de mensagens privadas;
- 7) aplicar-se-á a responsabilidade civil conforme do Código de Defesa do Consumidor para os provedores que funcionam como *marketplace*;
- 8) provedores devem criar normas internas sobre notificações, devido processo e relatórios anuais de transparência (autorregulação);
- 9) deverão ser criados canais de atendimento acessíveis, inclusivos, acessíveis e amplamente divulgados;
- 10) as normas internas deverão ser acessíveis ao público e revisadas periodicamente;
- 11) os provedores de aplicações de internet com atuação no Brasil devem ter sede e representante legal no país, com poderes para representar judicial e administrativamente, fornecer informações às autoridades e cumprir determinações judiciais e responder por sanções;
- 12) a responsabilidade dos provedores de aplicações de internet não é

objetiva em nenhum dos casos, sendo necessária a demonstração de culpa ou omissão;

- 13) necessidade de criação de legislação que supra as deficiências do art. 19 do Marco Civil da Internet.

Como se vê, apesar da exclusão dos ilícitos relacionados à honra pessoal, o Supremo Tribunal Federal posicionou-se pela inconstitucionalidade parcial do artigo 19 do Marco Civil da Internet privilegiando a adoção do modelo de *notice and take down*.

Logo, ainda que por vias reflexas, após mais de uma década de vigência do Marco Civil da Internet, um dos dispositivos que mais gerou controvérsias ao longo dos anos, é abandonado para que cerca de vinte e cinco anos após a publicação da Diretiva 2000/31/CE – que inclusive já é objeto de novas discussões –, o modelo de *notice and take down* seja adotado no Brasil.

Ao nosso ver, ao declarar a inconstitucionalidade parcial do artigo 19 do Marco Civil da Internet, privilegiando o sistema de *notice and take down*, o Supremo Tribunal Federal caminhou em direção acertada, apesar de tratar-se de matéria de competência do Poder Legislativo. Em especial, destaca-se a fixação do entendimento de que, apesar da aplicação do novo modelo, a responsabilidade dos provedores de internet é subjetiva e a presunção de responsabilidade ocorrerá apenas nos casos de impulsionamento pago ou em casos em que houver o uso de rede artificial de distribuição.

Aqui, destaca-se que embora seja desejável a responsabilização dos provedores de aplicações de internet em razão de uma conduta omissa, a imputação de um dever de vigilância poderia implicar uma oneração desproporcional dos provedores, além de lhes atribuir um poder de controle sobre conteúdos veiculados que não é próprio da ordem constitucional.

A hierarquização de direitos fundamentais viola a ordem constitucional e a imputação de responsabilidade objetiva aos provedores de aplicação de internet privilegiaria os direitos fundamentais dispostos no artigo 5º, *caput* e incisos X, XXVII e XXVIII da Constituição brasileira. A única exceção razoável seria nos casos de impulsionamento de conteúdo, hipótese em que é possível presumir que, uma vez atuando ativamente na divulgação de conteúdos, os provedores de aplicações de internet

tomam conhecimento de seu inteiro teor, podendo ser responsabilizados em razão de sua eventual ilicitude.

A conclusão adotada pelo Supremo Tribunal Federal, portanto, endereça e atualiza, de maneira adequada para o momento, um problema que há muito permeava as discussões em cenário nacional. A adoção da regra geral do sistema de *notice and take down* vai ao encontro das necessidades de uma maior regulação dos ambientes digitais no Brasil, à luz de medidas já adotadas em outros países.

Indo além, no mesmo sentido do entendimento que se formou no Supremo Tribunal Federal, a proposta apresentada pela Comissão de Juristas responsável pela revisão e atualização do Código Civil⁵² prevê a aplicação do regime de *notice and take down* no Brasil. Em uma sugestão de disposição acerca da moderação de conteúdo, consta a seguinte obrigação: “*demonstrado o conhecimento pela plataforma sobre a potencial ilicitude do conteúdo, mediante notificação eletrônica do interessado, deverão ser adotadas as providências necessárias para a indisponibilização do conteúdo ilícito*”.

Considerando que, no Brasil, as plataformas digitais (provedores de aplicações internet) possuem papel central no cotidiano dos brasileiros,⁵³ revisar o sistema de responsabilização previsto no artigo 19 do Marco Civil da Internet é medida que se impõe. A rápida dispersão de conteúdos, ainda que ilícitos e nocivos a terceiros, justifica a necessidade de uma atuação diligente por parte dos provedores de aplicações de internet.

Para viabilizar a adoção de tal sistema, cumpre aos provedores de aplicações de internet disponibilizar canais de fácil acesso e padronizados, permitindo a denúncia de conteúdo ilícito e, ainda, criando um sistema para que, em tempo razoável, as denúncias sejam analisadas e os conteúdos efetivamente ilícitos sejam retirados do ar.

52. Disponível em <<https://legis.senado.leg.br/atividade/comissoes/comissao/2630/>>, acesso em 28 dez. 2024.

53. PACETE, Luiz Gustavo. Brasil é o terceiro maior consumidor de redes sociais em todo o mundo. Disponível em <<https://forbes.com.br/forbes-tech/2023/03/brasil-e-o-terceiro-pais-que-mais-consome-redes-sociais-em-todo-o-mundo/>>, acesso em: 09 fev. 2025.

5. CONCLUSÃO

A internet é uma ferramenta global, em constante evolução e, assim sendo, as soluções jurídicas correspondentes também serão sempre objeto constante de mudança e adaptação. Nesse contexto, o regime de responsabilidade proposto pelo Marco Civil da Internet, em relação aos provedores de aplicações de internet, de acordo com o qual eles apenas se responsabilizariam em caso de inércia após determinação judicial acerca da remoção do conteúdo, não se revela o mais adequado.

A previsão legal acerca do tema, embora tenha sido criada com o intuito de proteção ao direito constitucionalmente garantido de liberdade de expressão, acaba por colocar em risco a tutela de outros direitos assegurados constitucionalmente, face ao prolongamento temporal da veiculação de conteúdo ilícito. Com efeito, vincular a solução do ilícito a uma determinação do Poder Judiciário, com todas as suas especificidades, significa caminhar em descompasso com o dinamismo característico das relações presentes na internet.

A exemplo da legislação e da jurisprudência internacionais, é necessário buscar uma solução que permita uma resposta à altura e na mesma velocidade para combater os conteúdos ilícitos veiculados pelos provedores de aplicações de internet. Isso, por si só, não implica a exigência de um dever geral de vigilância e de controle, mas, sim, a coibição de atos manifestamente ilícitos e veiculados em plataformas digitais sem qualquer controle e/ou responsabilidade dos provedores de aplicações de internet.

Neste sentido, a criação de um sistema que atribua responsabilidade aos servidores de aplicação de internet faz-se necessária à efetiva proteção de diversos direitos, como visto ao longo do presente artigo. Permitir a livre circulação e a manutenção de conteúdo ilícito até que haja uma determinação judicial de remoção representa, em muitos casos, a ineficácia na tutela do direito do ofendido, dados o alcance e a velocidade de propagação de conteúdo consentido pelo uso da internet.

Sob essa perspectiva, a adoção do modelo *notice and take down* para combater a veiculação de conteúdo ilícito produzido por terceiros, à luz do que vem ocorrendo na União Europeia, parece ser mais adequada.

Tal modelo não implica a responsabilização irrestrita do provedor de aplicações

de internet, mas permite identificar critérios a partir dos quais a sua omissão acarreta a sua responsabilização civil, independentemente da sua provocação pelo Poder Judiciário, garantindo maior eficácia à medida e, também, maior proteção ao direito do ofendido.

O modelo foi adotado recentemente no julgamento dos Temas 987 e 533 pelo Supremo Tribunal Federal, promovendo pela primeira vez no Brasil a inclusão, de forma mais eficaz, dos provedores de aplicações de internet no ciclo de responsabilização, em razão de conteúdos ilícitos por eles veiculados. Não se trata de uma responsabilização irrestrita, mas da fixação de parâmetros que permitam maior eficiência no combate à divulgação de conteúdos ilícitos.

A declaração de inconstitucionalidade parcial do artigo 19 do Marco Civil da Internet é medida desejável e aqui defendida, mas, por si só, não é suficiente, sendo necessária a adoção de um regime de responsabilização geral, pelo qual, mediante notificação da parte interessada, o provedor de aplicações de internet será responsabilizado por deixar de indisponibilizar conteúdo ilícito. Para tanto, cumpre agora ao Poder Legislativo avançar na consolidação da matéria.

É apenas diante do estabelecimento do sistema proposto que, uma vez garantidas maiores segurança jurídica e objetividade ao tratamento da questão, que será possível evoluir na discussão sobre a matéria, de modo a abarcar a aplicação de sistemas mais complexos, tal como o sistema de *notice and stay down*.

REFERÊNCIAS

- ANGELOPOULOS, Christina; SMET, Stijn. Notice-and-Fair-Balance: How to reach a compromise between fundamental rights in european intermediary liability. *Journal of media law*, vol. 8, 2016.
- BARRETO JUNIOR, I. F.; FERREIRA LEITE, B. S. Responsabilidade civil dos provedores de aplicações por ato de terceiro na lei 12.965/14 (marco civil da internet). *Revista brasileira de estudos políticos*, v. 115, 27 nov. 2017.
- BONAVIDES, Paulo. *Curso de direito constitucional*. 14ª ed. São Paulo: Malheiros, 2004.
- BRASIL. *Constituição da República Federativa do Brasil de 1988*. Diário Oficial da União de 05.10.1988, Brasília, DF. Disponível em <https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>, acesso em: 29 dez. 2024.
- BRASIL. *Lei nº 10.406 de 10 de janeiro de 2002*. Institui o Código Civil. Diário Oficial da União de

- 11.02.2002, Brasília, DF. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/2002/110406compilada.htm>, acesso em 09 de fev. 2025.
- BRASIL. *Lei n. 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União de 24.04.2014, Brasília, DF. Disponível em <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/12965.htm>, acesso em: 29 dez. 2024.
- BRASIL. Supremo Tribunal Federal. *Tema 987*. Disponível em: <<https://portal.stf.jus.br/jurisprudenciaRepercussao/verAndamentoProcesso.asp?incidente=5160549&numeroProcesso=1037396&classeProcesso=RE&numeroTema=987>>, acesso em: 30 dez. 2024.
- BRASIL. Supremo Tribunal Federal. *Tema 533*. Disponível em: <<https://portal.stf.jus.br/jurisprudenciaRepercussao/verAndamentoProcesso.asp?incidente=5217273&numeroProcesso=1057258&classeProcesso=RE&numeroTema=533>>, acesso em: 30 dez. 2024.
- BRASIL. Supremo Tribunal Federal. RE 1037396. Recorrente: Facebook Serviços Online do Brasil Ltda., Recorrida: Lourdes Pavioto Correa. Relator: Ministro Dias Toffoli, 01 de março de 2018. Disponível em: <<https://jurisprudencia.stf.jus.br/pages/search/repercussao-geral9662/false>>, acesso em 13 fev. 2025.
- BREGA, Gabriel. A regulação de conteúdo nas redes sociais: uma breve análise comparativa entre o NetzDG e a solução brasileira. *Revista direito gv*, v. 19, e2305, São Paulo, 2023.
- BUITEN, Miriam. The digital services act from intermediary liability to platform regulation. *12 journal of intellectual property, information and technology and electronic commerce law*, 2021.
- CARVALHO, Luísa. *Toffoli afirma que artigo 19 do Marco Civil da Internet é inconstitucional*. JOTA. Disponível em <<https://www.jota.info/stf/do-supremo/toffoli-afirma-que-artigo-19-do-marco-civil-da-internet-e-inconstitucional>>, acesso em: 04 jan. 2025.
- CARVALHO, Luísa. *Ponto a ponto: entenda o voto de barroso sobre o artigo 19 do marco civil da internet*. JOTA. Disponível em <<https://www.jota.info/stf/do-supremo/ponto-a-ponto-entenda-o-voto-de-barroso-sobre-o-artigo-19-do-marco-civil-da-internet>>, acesso em: 04 jan. 2025.
- CARVALHO, Mario Cesar. *Dias Toffoli faz voto de lunático para regular a internet*. Poder 360. <<https://www.poder360.com.br/futuro-indicativo/dias-toffoli-faz-voto-de-lunatico-para-regular-a-internet/>>, acesso em: 04 jan. 2025.
- CASTRO, Carla Frade de Paula. Responsabilidade civil dos provedores de aplicações de internet por infrações de terceiros a direitos autorais. *Revista de informação legislativa*, v. 60, n. 237, p. 141-171, jan./mar. 2023.
- GODOY, Claudio Luiz Bueno de. Uma análise crítica da responsabilidade civil dos provedores na Lei n. 12.965/14 (Marco Civil da Internet). In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). *Direito & internet III –Tomo II: marco civil da internet (Lei n. 12.965/2014)*. São Paulo: Quartier Latin, 2015.

IPPOLITO, Fulvio Sarzana Di S. *I contratti di internet e del commercio elettronico*, Milano: A. Giuffrè Editore, 2001.

KUCZERAWY, Aleksandra. From 'notice and take down' to 'notice and stay down': risks and safeguards for freedom of expression. In: Giancarlo Frosio (ed) *The Oxford handbook of intermediary liability online*, 2019. Disponível em: <<https://ssrn.com/abstract=3305153>>, acesso em: 04 jan. 2025.

LEONARDI, Marcel. *Responsabilidade civil dos provedores dos serviços de internet*. São Paulo: Juarez de Oliveira, 2005, e-book.

LEONARDI, Marcel. *Cem motivos para o STF preservar o artigo 19*. Estadão. Disponível em <<https://www.estadao.com.br/opiniao/espaco-aberto/cem-motivos-para-o-stf-preservar-o-artigo-19/?srsltid=AfmBOoqHMtbvRaCZxUNUCz15jv2S69lUrpy0KT6AqzpeWiacIngj0He1>>, acesso em 03 jan. 2025.

MANTELERO, Alessandro. *Diritto dell'informatica*. Milano: UTET, 2014.

MIRAGEM, Bruno. Direito civil. *Responsabilidade civil*. São Paulo: Saraiva, 2015.

PACETE, Luiz Gustavo. Brasil é o terceiro maior consumidor de redes sociais em todo o mundo. Disponível em <<https://forbes.com.br/forbes-tech/2023/03/brasil-e-o-terceiro-pais-que-mais-consome-redes-sociais-em-todo-o-mundo/>>, acesso em: 09 fev. 2025.

SARLET, Ingo Wolfgang. Liberdade de expressão e biografias não autorizadas — notas sobre a ADI 4.815. Consultor Jurídico. 19 de junho de 2015. Disponível em: <<https://www.conjur.com.br/2015-jun-19/direitos-fundamentais-liberdade-expressao-biografias-nao-autorizadas>>, acesso em: 02 fev. 2025.

SCHREIBER, Anderson; RIBAS, Felipe; MANSUR, Rafael. *Deepfakes: regulação e responsabilidade civil*. In: TEPEDINO, Gustavo; SILVA, Rodrigo da Guia (Coord.). O direito civil na era da inteligência artificial. São Paulo: Thomson Reuters Brasil, 2020.

SCHREIBER, Anderson. Marco civil da internet: avanço ou retrocesso? A responsabilidade civil por dano derivado do conteúdo gerado por terceiro. In: LUCCA, Newton de; SIMÃO FILHO; Adalberto; LIMA, Cíntia Rosa Pereira de (Coords). *Direito & internet III - Tomo II: marco civil da internet* (Lei nº 12.965/2014). São Paulo: Quartier Latin, 2015.

SILVA, Alberto Jacob Cerda. Chile. In: Dumortier, Jos; Gryffroy, Pieter; Roex, Ruben; Van Der Sype, Yung Shin (eds.), *IEL privacy and technology law*. Kluwer law international bv, Netherlands, 2020.

SOUZA, Carlos Affonso Pereira de. As cinco faces de proteção à liberdade de expressão no marco civil da internet. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coord.). *Direito & internet III: marco civil da internet. Tomo II*. São Paulo: Quartier Latin, 2015.

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

STOCO, Rui. *Tratado de responsabilidade civil*. 6. ed. São Paulo: RT, 2004.

TEFFÉ, Chiara; SOUZA, Carlos Affonso. Responsabilidade civil dos provedores na rede: análise da aplicação do marco civil da internet pelo Superior Tribunal de Justiça. *Revista IBERC*, Minas Gerais, v.1, n.1, p. 01-28, nov.-fev./2019.

TEFFÉ, Chiara; MORAES, Maria Celina. Redes sociais virtuais: privacidade e responsabilidade civil. Análise a partir do marco civil da internet. *Pensar - Revista de ciências jurídicas*, 22(1), 108-46. 2017.

UNIÃO EUROPEIA. *Diretiva 2000/31/CE do Parlamento Europeu e do Conselho*, relativa a certos aspectos legais dos serviços da sociedade de informação, em especial do comércio electrónico, no mercado interno («Directiva sobre o comércio electrónico»), 08 jun. 2000. Disponível em: <<https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex%3A32000L0031>>, acesso em: 01 jan. 2025.

UNIÃO EUROPEIA. Acórdão do Tribunal de Justiça (Grande Secção) de 23 de março de 2010. *Google France SARL and Google Inc. v Louis Vuitton Malletier SA*, C-236/08, ECLI:EU:C:2010:159. Disponível em: <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62008CJ0236>>, acesso em 02 jan. 2025.

UNIÃO EUROPEIA. Acórdão do Tribunal de Justiça (Grande Secção) de 12 de julho de 2011. *L'Oréal SA and Others v eBay International AG and Others*, C-324/09. ECLI:EU:C:2011:474. Disponível em: <<https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A62009CJ0324>>, acesso em 02 jan. 2025.

UNIÃO EUROPEIA. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho*. Regulamento Geral sobre a Proteção de Dados, 27 abr. 2016. Disponível em: <<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>>, acesso em: 09 fev. 2025.

UNIÃO EUROPEIA. *Regulamento (UE) 2022/2065 do Parlamento Europeu e do Conselho*, relativo a um mercado único para os serviços digitais e que altera a Diretiva 2000/31/CE, 19 out. 2022. Disponível em: <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065>>, acesso em: 01 jan. 2025.

UNIÃO EUROPEIA. *Diretiva 2019/790 do Parlamento Europeu e do Conselho*, relativa aos direitos de autor e direitos conexos no mercado único digital e que altera as Diretivas 96/9/CE e 2001/29/CE, 17 abr. 2019. Disponível em: <<https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX:32019L0790>>, acesso em: 01 jan. 2025.

VAINZOF, Rony. Da responsabilidade por danos decorrentes de conteúdos gerados por terceiros. In MASSO, F. del; ABRUSIO, J.; FLORÊNCIO FILHO, Marco A. (Coord.). *Marco civil da internet: Lei 12.965/2014*. São Paulo: RT, 2014.

VALENTE, Mariana Giorgetti. Direito autoral e plataformas de internet: um assunto em aberto. *InternetLab*, 18 abr. 2019. Disponível em: <<https://internetlab.org.br/pt/especial/direito-autoral-e-plataformas-de-internet-um-assunto-em-aberto/>>, acesso em: 04 jan. 2025.

ZURTH, Patrick. The German NetzDG as Role Model or Cautionary Tale? Implications for the

Debate on Social Media Liability. *Fordham Intellectual Property, Media and Entertainment Law Journal*. 31 Fordham Intell. Prop. Media & Ent. L.J. 1084 (2021). Disponível em: <<https://ir.law-net.fordham.edu/iplj/vol31/iss4/4>>, acesso em: 09 fev. 2025.

ENTRE A LIBERDADE DE EXPRESSÃO E A CENSURA NA ERA DIGITAL: UMA ANÁLISE DO ARTIGO 19 DO MARCO CIVIL DA INTERNET

Eduardo Serra Rossigneux Vieira

Professor de Direito Empresarial. Sócio Fundador do Vieira e Serra Advogados.

Carolina Adler Cendron

Pós-graduada pelo Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP).

Pesquisadora do Laboratório de Governança e Regulação de Inteligência Artificial (Lia.IDP). Advogada no Vieira e Serra Advogados.

DOI: <https://doi.org/10.59224/dti7.ch11>

Resumo: A presente pesquisa analisa a eficácia do art. 19 do Marco Civil da Internet (MCI) e as possíveis implicações de eventual declaração de inconstitucionalidade para os direitos e garantias dos usuários dentro das plataformas.

Palavras-chave: Marco Civil da Internet; Liberdade de expressão; Responsabilidade do provedor de aplicação.

Abstract: *This research analyzes the effectiveness of Article 19 of the Brazilian Civil Rights Framework for the Internet and the possible implications of the likely declaration of unconstitutionality for the Internet for the rights and guarantees of users within the platforms.*

Keywords: *Civil Rights Framework for the Internet. Freedom of expression; Application provider liability.*

SUMÁRIO: 1. Introdução; 2. O Marco Civil da Internet e o art 19; 3. Os desafios e proteções legais do direito fundamental da liberdade de expressão na internet; 4. Moderação de conteúdo e responsabilidade dos provedores de aplicação; 5. Reanálise da constitucionalidade do art. 19 do Marco Civil da Internet: Julgamento conjunto do Tema 987 e Tema 533 do Supremo Tribunal Federal; 6. As possíveis implicações em caso de ser declarada a inconstitucionalidade do art. 19 para a liberdade de expressão on-line; 7. Conclusão; Referências.

1. INTRODUÇÃO

A ascensão da internet e das redes sociais transformou profundamente as dinâmicas da comunicação, ampliando o acesso à informação e redefinindo os limites da liberdade de expressão. No Brasil, a necessidade de um marco regulatório para a governança digital levou à sanção da Lei n. 12.965/2014, chamada Marco Civil da Internet (MCI). Essa lei que estabeleceu princípios e regras para a utilização da rede e colocou em equilíbrio direitos de ordem individual e interesses coletivos.

Entre seus dispositivos, um dos mais controversos é o art. 19, que dispõe que provedores¹ de aplicação de internet somente poderão vir a ser responsabilizados por conteúdos gerados por terceiros após decisão judicial específica que determine a exclusão de determinada postagem. Essa redação teve por objetivo garantir um ambiente digital no qual predominassem a liberdade de expressão, a proibição de mecanismos de censura prévia, e a vedação ao anonimato.

Entretanto, decorridos dez anos desde a sua entrada em vigor, a norma vem sofrendo críticas, de modo que, atualmente, o Supremo Tribunal Federal julga a constitucionalidade do art. 19 do MCI², no âmbito do Tema 987 e Tema 533 de Repercussão Geral, o que pode reconfigurar o modelo de responsabilidade civil dos provedores de aplicação³ no país.

-
1. Nos termos do Superior Tribunal de Justiça: “os provedores de serviços de internet são aqueles que oferecem serviços ligados ao funcionamento dessa rede mundial de computadores, ou por meio dela. Trata-se de gênero do qual são espécies as demais categorias, como: (i) provedores de backbone (espinha dorsal), que detêm estrutura de rede capaz de processar grandes volumes de informação. São os responsáveis pela conectividade da Internet, oferecendo sua infraestrutura a terceiros, que repassam aos usuários finais acesso à rede; (ii) provedores de acesso, que adquirem a infraestrutura dos provedores de backbone e revendem aos usuários finais, possibilitando a estes conexão com a Internet; (iii) provedores de hospedagem, que armazenam dados de terceiros, conferindo-lhes acesso remoto; (iv) provedores de informação, que produzem as informações divulgadas na Internet; e (v) provedores de conteúdo, que disponibilizam na rede os dados criados ou desenvolvidos pelos provedores de informação ou pelos próprios usuários da web”. BRASIL. Superior Tribunal de Justiça. Recurso Especial 1316921/RJ. Relator: Min. Nancy Andrighi. Julgado em: 26 jun. 2012.
 2. Este artigo é escrito em março de 2025, antes, portanto, do julgamento.
 3. Existem dois tipos principais de provedores, de acordo com o MCI. O provedor de conexão é aquele que possibilita que o usuário tenha acesso a rede. Por outro lado, o provedor de aplicação

A ser assim, uma eventual declaração de inconstitucionalidade desse artigo significaria uma mudança substancial da balança da proteção da liberdade de expressão.

Em que pese haja a pretensão da desejável atenuação dos impactos dos conteúdos nocivos, há o risco oculto de estabelecer um grau excessivo de moderação, de modo a inibir indevidamente as manifestações livres, culminando em censura.

Nesse cenário, o presente estudo procura responder ao seguinte questionamento: em que medida o art. 19 do MCI cumpriu seu objetivo de proteger a liberdade de expressão ao delimitar a responsabilidade dos provedores de aplicação e coibir o anonimato, na última década, e como uma eventual declaração de inconstitucionalidade pelo STF poderia transformar esse cenário no Brasil?

Para responder ao problema apresentado, é adotada uma abordagem dedutiva, qualitativa e exploratória, centrada na revisão bibliográfica e na análise normativa. O método dedutivo é adotado a partir de premissas gerais sobre o direito fundamental da liberdade de expressão e governança digital, para avançar até a avaliação do art. 19 do MCI e de suas implicações. A pesquisa qualitativa se justifica na medida em que é necessário interpretar normas jurídicas e doutrina. Além disso, é uma pesquisa exploratória, uma vez que se volta para os impactos regulatórios do art. 19 do MCI e as eventuais consequências de eventual declaração de inconstitucionalidade pelo STF.

No decorrer da pesquisa, será analisado o contexto normativo do MCI, as bases da responsabilidade civil das plataformas, os desafios da moderação de conteúdo e as possíveis repercussões em caso de reinterpretação judicial do art. 19.

é aquele que permite o acesso do usuário em um canal de comunicação. Nesse sentido, elucida o MCI: Art. 5º Para os efeitos desta Lei, considera-se: (...) V - conexão à internet: a habilitação de um terminal para envio e recebimento de pacotes de dados pela internet, mediante a atribuição ou autenticação de um endereço IP; (...) VII - aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet; (...). BRASIL. Lei nº 12.965, de 23 de abril de 2014: estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

2. O MARCO CIVIL DA INTERNET E O ARTIGO 19

Antes de analisar o art. 19 do Marco Civil da Internet (MCI) e sua eficácia ao longo da última década, faz-se necessário traçar um panorama histórico anterior à sanção da lei. Esse resgate contextual permite compreender o cenário da época e, consequentemente, as motivações subjacentes à elaboração do texto legal.

O debate nos remete ao início dos anos sessenta, quando a comunicação em rede era restrita aos departamentos de segurança e às forças armadas dos Estados Unidos da América, sendo, então principalmente utilizada para fins estratégicos e de defesa nacional.⁴

A disponibilização da internet à população civil, ainda que de forma precária, teve início na década de oitenta, quando passou a ser oferecida para o meio acadêmico, mas ainda de forma muito restrita, à época, o principal objetivo era apenas a troca de informações por meio de códigos e protocolos conhecidos apenas por um grupo de especialistas envolvidos.⁵

Somente na década de noventa ocorreu, de fato, a revolução no uso da internet quando, impulsionada pelo barateamento equipamentos, tornou-se mais acessível, o que fomentou o crescimento e interesse em sua utilização por parte da sociedade civil.

Surgiu, assim, a nova concepção da internet como uma rede global de computadores, uma vez que transpõe limites geográficos e culturais ao possibilitar a comunicação instantânea entre os usuários.⁶

Nesse cenário de ascensão da tecnologia, os Estados Unidos da América (EUA) tomaram a dianteira ao buscar realizar uma regulamentação de comunicações telefônicas e da internet. Diante disso, elaboraram a *Communications Decency Act (CDA) of 1996*, uma legislação cujo principal objetivo era combater os conteúdos ilícitos, em especial, a disseminação de conteúdos pornográficos.⁷

4. TEIXEIRA, Tarcisio. *Direito Digital e Processo Eletrônico*. 7. ed. São Paulo: SaraivaJur, 2023. p. 3.

5. *Ibidem*.

6. *Idem*, p. 5.

7. UNITED STATES. *Communications Decency Act of 1996*. S. 314, 104th Congress.

A introdução da Seção 230⁸ do CDA é considerada, até hoje, uma das partes mais significativas, pois ao conceder imunidade aos provedores de serviços on-line em relação ao conteúdo compartilhado por terceiros em suas plataformas, desempenhou um papel crucial na elaboração de legislações subsequentes em vários países, incluindo o Brasil.

À medida que os EUA avançavam em matéria de regulação da internet, o Brasil enfrentava uma situação precária quanto à sua normatização. Esta omissão legislativa criava um ambiente de incerteza e insegurança jurídica na proteção dos usuários brasileiros na esfera digital, fazendo prevalecer uma percepção generalizada de que a internet era uma "terra sem lei", em que as atividades dos usuários podiam ser exercidas sem consequências ou responsabilizações.

Durante este período de ausência de regulamentação, coube ao Superior Tribunal de Justiça (STJ) o dever de estabelecer parâmetros para o combate dos ilícitos virtuais e o nível de responsabilidade das plataformas digitais.⁹

Além disso, naquele período, o ecossistema da internet era composto por um número reduzido de empresas, muitas ainda em estágios iniciais e com fragilidades financeiras e operacionais. Nesse contexto, a possibilidade de responsabilização objetiva das plataformas por meio de ações judiciais representava uma ameaça à continuidade de suas operações.

Frente a esta situação, as iniciativas legais da época procuravam, não apenas proteger os direitos e a defesa dos usuários, mas promover, igualmente, o desenvolvimento e o fortalecimento das empresas do setor digital. Por consequência, essa abordagem dupla visava a criação de um ambiente propício ao desenvolvimento de uma rede cada vez mais extensa e forte de conectividade on-line entre os cidadãos.

Foi essa congruência de esforços que viabilizou o cenário atual: uma rede interligada e universal de computadores, na qual uma parcela relevante da população mundial está ligada de forma ininterrupta.

No Brasil, contudo, um evento ocorrido em maio de 2011 serviu como catalisador

8. UNITED STATES. Communications Decency Act of 1996. S. 340, 104th Congress.

9. ANDRIGHI, Nancy. Marco Civil da Internet. *Entrevistada pelo jornal Migalhas*, 2013. Disponível em: <https://www.youtube.com/watch?v=-DultHob9Gg&t=52s>.

para as discussões a respeito da necessidade de uma regulamentação específica para o ambiente digital. Naquele episódio, a atriz Carolina Dieckmann foi vítima de um ataque cibernético em que seu computador particular foi invadido por um hacker. O infrator, em posse de informações e arquivos privados da atriz, tentou extorqui-la, ameaçando divulgar suas fotos íntimas na internet caso não recebesse determinada quantia. Diante da recusa, as imagens foram publicadas na rede.¹⁰

Esse evento gerou grande repercussão pública e evidenciou a necessidade urgente de se criar mecanismos legais de proteção à privacidade e à intimidade no espaço virtual, o que resultou na sanção da Lei n. 12.737/2013, comumente conhecida como “Lei Carolina Dieckmann”.¹¹

O caso da atriz Carolina Dieckmann demonstrou de maneira clara a urgente necessidade da criação de uma legislação específica para regular o ambiente digital brasileiro, pois o episódio não apenas escancarou a vulnerabilidade do meio digital, como, também, gerou uma preocupação na população em torno da proteção dos seus direitos na internet, em especial no tocante à proteção da privacidade e da intimidade dos usuários.

Foi neste contexto de grande inquietação da sociedade e de urgência regulatória que foi sancionada a Lei n. 12.737/2013 como resposta à demanda de normatização do uso da internet no país. Sua confecção teve um processo inovador e participativo por meio de uma plataforma on-line em que toda a sociedade teve a oportunidade de participar dos acalorados debates, na busca de reunir as vozes e visões de diversos setores da sociedade brasileira.¹²

No final da fase de intenso debate público, o Projeto de Lei n. 2.126/2011¹³ foi

10. SENADO FEDERAL. *Dez anos de vigência da Lei Carolina Dieckmann: a primeira a punir crimes cibernéticos*. 2023. Disponível em: <https://www12.senado.leg.br/radio/1/noticia/2023/03/29/dez-anos-de-vigencia-da-lei-carolina-dieckmann-a-primeira-a-punir-crimes-ciberneticos>.

11. SENADO FEDERAL. Lei nº 12.737, de 30 de novembro de 2012: altera o Código Penal para tipificar crimes cometidos por meio da informática e dá outras providências. 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm.

12. SOUZA, Carlos Affonso; LEMOS, Ronaldo. *Marco Civil da Internet: construção e aplicação*. São Paulo: Editora Associada, 2016. p. 13-14.

13. CÂMARA DOS DEPUTADOS. PL 2126/2011. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=517255>.

submetido ao exame do Poder Executivo e do Congresso, assim o texto final foi sancionado pela Presidente da República resultando na promulgação da Lei n. 12.965/2014, conhecida como Marco Civil da Internet - MCI¹⁴. Assim, o MCI se firmou como uma norma reguladora de suma importância, consagrando princípios, garantias, direitos e obrigações sobre o uso da rede mundial no Brasil.

Embora o MCI esteja preocupado em assegurar uma ampla proteção a uma série de direitos fundamentais no ambiente de interação digital, é bom notar que foi dada uma atenção especial à proteção da liberdade de expressão, uma vez que coloca este direito fundamental em foco e traz garantias consistentes contra qualquer forma de censura prévia por parte das plataformas digitais.¹⁵

Nada obstante, o MCI também trouxe um importante mecanismo de responsabilização ao coibir o anonimato pelos usuários responsáveis pelas postagens. Assim, embora a liberdade de expressão fosse protegida, esta não pode ser exercida sem limites, especialmente quando utilizada para ferir outros direitos fundamentais.¹⁶

Nesse contexto, o art. 19 buscou impedir que provedores fossem responsabilizados por conteúdos de terceiros, uma vez que não foram eles que realizaram a postagem, mas somente abriram acesso ao meio digital, ao passo que também exigiu meios para identificação dos usuários que praticassem ilícitos.

Esse equilíbrio tem sido um dos pilares da regulamentação da internet no Brasil, mas também tem gerado controvérsias, especialmente quanto à eficácia do modelo adotado e aos desafios na identificação de infratores.

Nesse sentido, o MCI atendeu à necessidade de regulamentação da internet no Brasil, pois, ao proporcionar uma Lei que equilibrasse os interesses divergentes conseguiu assegurar o direito fundamental da liberdade de expressão e permitir a responsabilização daqueles que cometiam atos ilícitos, sem que a responsabilidade

14. BRASIL. *Lei nº 12.965, de 23 de abril de 2014: estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil*. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

15. SOUZA, Carlos Affonso; LEMOS, Ronaldo. *Marco Civil da Internet: construção e aplicação*. São Paulo: Editora Associada, 2016, p. 15-16.

16. Ibidem.

da publicação recaísse sobre o provedor de aplicação. Ademais, conseguiu aproximar a população do Poder Judiciário que tomou o papel principal de assegurar os direitos dos usuários contra ilícitos cometidos na esfera virtual.

Outrossim, o art. 19 do MCI¹⁷, em particular, constitui um ponto fundamental da regulação da responsabilização dos provedores de aplicações de internet, pois consagra que as plataformas não têm o dever de realizar controle prévio das publicações realizadas por seus usuários, sendo que a responsabilidade pela remoção de determinado conteúdo somente emerge após uma decisão judicial nesse sentido.

A exceção fica prevista no art. 21¹⁸, que estabelece que nos casos de divulgação não autorizada de imagens de nudez ou atos sexuais de natureza privada o provedor de aplicação deve remover o conteúdo imediatamente, mediante notificação da pessoa afetada, independentemente de ordem judicial.

Essa exceção reflete a necessidade de uma remoção ágil, especialmente diante de violações à dignidade da pessoa humana, como na exposição não consentida de imagens íntimas, nos rememorando que a legislação surgiu como uma resposta direta ao caso da atriz Carolina Dieckmann.

Outro elemento essencial do MCI é a responsabilização legal que assegura que

17. BRASIL. *Lei nº 12.965, de 23 de abril de 2014: estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil*. Art. 19. "Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário." Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

18. BRASIL. *Lei nº 12.965, de 23 de abril de 2014: estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil*. Art. 21. "O provedor de aplicações de internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo." Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

usuários responsáveis pela veiculação de postagens ofensivas ou ilícitas possam ser identificados pelos provedores de conexão, por meio de seus dados de registro, usualmente designados como endereço IP, definido como “*o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais*”.¹⁹

A possibilidade dessa identificação opera como um importante fator de dissuasão de comportamentos abusivos, tendo em vista que ao se estipular que as práticas realizadas on-line podem ser perseguidas e atribuídas a pessoas específicas, a legislação inibe a realização de atos ilícitos que muitas vezes prosperam no seio de uma falsa sensação de anonimato. Com isso, o MCI, ao mesmo tempo em que favorece a retenção de um ambiente on-line mais seguro e responsável, não inviabiliza a liberdade de expressão que é essencial para a formação de uma sociedade democrática e pluralista na era digital.

Nos termos de Carlos Affonso e Ronaldo Lemos “*foi com essa motivação que o Marco Civil foi concebido: como uma lei que pudesse preservar as bases para a promoção das liberdades e dos direitos da internet no Brasil*”, de modo que foi criada uma regulação com base primordial nos direitos humanos, afastando uma eventual regulação repressiva da rede.²⁰

Nesse contexto, o MCI surge como uma norma que procura equilibrar diversos interesses e direitos. De um lado, apresenta uma preocupação coletiva com o desenvolvimento e o crescimento de plataformas digitais, levando em consideração seu relevante papel na economia e na sociedade contemporâneas. De outro lado, impõe robustas salvaguardas para garantir o direito dos usuários no mundo on-line, com um forte enfoque na liberdade de expressão.²¹

19. BRASIL. Lei nº 12.965, de 23 de abril de 2014: estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Art. 5, III. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

20. SOUZA, Carlos Affonso; LEMOS, Ronaldo. *Marco Civil da Internet: construção e aplicação*. São Paulo: Editora Associada, 2016, p. 16.

21. SOUZA, Carlos Affonso; LEMOS, Ronaldo. *Marco Civil da Internet: construção e aplicação*. São Paulo: Editora Associada, 2016, p. 16.

3. OS DESAFIOS E PROTEÇÕES LEGAIS DO DIREITO FUNDAMENTAL DA LIBERDADE DE EXPRESSÃO NA INTERNET

A liberdade de expressão configura um dos alicerces do Estado Democrático de Direito, sendo a sua razão de ser tanto para a autorrealização do indivíduo quanto para a sua operacionalização nos quadros da democracia, pois é por meio da liberdade de expressão que o cidadão comunica as suas ideias e exprime suas opiniões.²²

Como elucida o Professor Paulo Gonet Branco, as liberdades são proclamadas partindo-se de esfera da pessoa do homem em busca da autorrealização pela exteriorização do ser para os outros. A ser assim, o Estado democrático tem uma justificativa que é um meio para que estas liberdades se vejam protegidas, ao tomar uma posição defensiva, pois não tomará nenhuma medida para impedir a liberdade de expressão até que seja manifestada e verificada sua irregularidade.²³

Daniel Sarmiento ressalta a importância da liberdade de expressão para a democracia ao argumentar que para que seja efetivada os cidadãos devem ter amplo acesso a informações e a diversificação de ponto de vistas, a fim de que possam formar as suas próprias convicções.²⁴

Frisa-se que Constituição Federal de 1988, expressamente, protege o direito à liberdade de expressão, sendo essa proteção consagrada em diversos dispositivos, incluindo-se, por exemplo, no art. 5º, inciso IV, que estabelece que “*é livre a manifestação do pensamento, sendo vedado o anonimato*”, e no art. 220, que diz que “*A manifestação do pensamento, a criação, a expressão e a informação, sob qualquer forma, processo ou veículo não sofrerão qualquer restrição, observado o disposto nesta Constituição*”, onde se elucida, ainda, os §§ 1º e 2º com os seguintes termos: “*Nenhuma lei conterá dispositivo que possa constituir embaraço à plena liberdade de*

22. MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. *Curso de Direito Constitucional*. 12. ed. São Paulo: SaraivaJur, 2017. p. 263.

23. MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. *Curso de Direito Constitucional*. 12. ed. São Paulo: SaraivaJur, 2017. p. 267.

24. SARMENTO, Daniel. Comentário ao artigo 5º, inciso IV. In: CANOTILHO, J. J. Gomes; MENDES, Gilmar F.; SARLET, Ingo W.; STRECK, Lenio L. (coord.). *Comentários à Constituição do Brasil*. São Paulo: Saraiva/Almedina, 2013, p. 255.

*informação jornalística em qualquer veículo de comunicação social, observado o disposto no art. 5º, IV, V, X, XIII e XIV” e “É vedada toda e qualquer censura”.*²⁵

Portanto, o Estado deve garantir que a liberdade de expressão seja preservada em

sua plenitude, enquanto não haja colisão com os demais direitos fundamentais ou com os valores constitucionais, ou seja, a liberdade de expressão, que é um direito fundamental, impõe ao Estado um dever de não ingerência ou um dever de não censurar.²⁶

Dito isso, há que se ter que a censura se manifesta como qualquer forma de controle prévio sobre o conteúdo das manifestações individuais – verbais ou não verbais -, dessa forma, antes mesmo de ser verificada sua eventual irregularidade, já se determina a remoção, sem espaço para uma discussão crítica.

É necessário compreender, ainda, que ao Estado não compete determinar o que se pode ou não dizer, mas sim ao público que sofre a opinião manifestada cabe exercitar seu juízo crítico.²⁷

Nesta conjuntura, com o propósito de proteger o direito à liberdade de expressão, o MCI adotou uma postura de contenção quanto à responsabilidade das aplicações da internet.

Para tanto, a lei estabeleceu que essas plataformas de aplicação não são, de modo geral, responsáveis pelo conteúdo publicado por terceiros, incutindo no Judiciário o poder decisório a respeito do que deveria ou não ser excluído do mundo virtual, o que resultaria na objeção da censura prévia e que a legalidade dos conteúdos on-line seja analisada pelas autoridades competentes, em decorrência de um processo devido.

Conforme destacado pelo Professor Carlos Affonso Pereira de Souza, o MCI conferiu um tratamento privilegiado ao direito fundamental da liberdade de expressão, visto que a Lei menciona a garantia deste direito, ao menos, em cinco

25. MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. *Curso de Direito Constitucional*. 12. ed. São Paulo: SaraivaJur, 2017. p. 268.

26. MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. *Curso de Direito Constitucional*. 12. ed. São Paulo: SaraivaJur, 2017. p. 268.

27. MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. *Curso de Direito Constitucional*. 12. ed. São Paulo: SaraivaJur, 2017. p. 269.

momentos fundamentais.²⁸ Inicialmente, o MCI consagra, em seu art. 2º,²⁹ como a liberdade de expressão como fundamento do uso da internet no Brasil, e o art. 3º reafirma que este é um dos princípios que a governam.³⁰ O art. 8º³¹ também estabelece, ainda, que a garantia do direito à privacidade e da liberdade de expressão nas comunicações é condição de exercício pleno do direito de acesso à internet, o que promove uma conexão intrínseca entre a liberdade de expressão e o próprio direito de acesso à internet.³²

Nesse contexto, a proteção conferida à liberdade de expressão pelo MCI pode levantar questionamentos como: qual seria a relação entre a responsabilidade do provedor de aplicação sobre a remoção de conteúdos publicados por terceiros e o direito fundamental à liberdade de expressão?

O art. 19 do MCI oferece uma resposta a essa pergunta ao dispor que os provedores de aplicação somente poderão ser responsabilizados civilmente por danos causados por conteúdos de terceiros caso descumpram ordem judicial específica para remoção da publicação considerada ilícita. O dispositivo deixa claro que esta regra foi estabelecida "*com o intuito de assegurar a liberdade de expressão e*

28. SOUZA, Carlos Affonso Pereira de. *As cinco faces da proteção à liberdade de expressão no Marco Civil da Internet*. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio (ITS Rio), 2018. Disponível em: https://itsrio.org/wp-content/uploads/2018/06/as_cinco_faces.pdf.

29. BRASIL. *Lei nº 12.965, de 23 de abril de 2014: estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil*. Art. 2º A disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão (...). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

30. BRASIL. *Lei nº 12.965, de 23 de abril de 2014: estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil*. Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios: I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal (...). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

31. BRASIL. *Lei nº 12.965, de 23 de abril de 2014: estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil*. Art. 8º A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet. (...). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

32. SOUZA, Carlos Affonso Pereira de. *As cinco faces da proteção à liberdade de expressão no marco civil da internet*, Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio (ITS Rio), 2018, p.2. Disponível em: https://itsrio.org/wp-content/uploads/2018/06/as_cinco_faces.pdf.

impedir a censura", inclusive.³³

Na elaboração da norma, havia a preocupação de que certas responsabilidades atribuídas aos provedores de aplicação gerariam um dever aumentativo de fiscalização por parte das plataformas, de modo que eliminariam rapidamente as novas postagens que pudessem ter qualquer indício de ilegalidade, já que não gostariam de ser responsabilizadas. Essa retirada imediata do conteúdo, portanto, geraria uma lesão ao direito à liberdade de expressão, uma vez que a manifestação do usuário seria retirada sem possibilidade de contraditório.

De tal maneira, sem a imediata responsabilização do provedor de aplicação pelos conteúdos postados por terceiros, haveria, a favor destes, uma supervisão branda neste sistema de postagens, o que iria propiciar a liberdade de expressão. Da mesma forma, se a pessoa se sentisse lesada em seus direitos, poderia notificar a plataforma e procurar o Judiciário para assegurar o seu direito que foi violado pela expressão do outro, uma vez que a pessoa do ofensor estaria identificada pelo provedor de acesso.

Em atenção à proteção da liberdade de expressão, que não deve ser restringida até que se constate a violação de outro direito fundamental, o Marco Civil da Internet (MCI) não atribui às plataformas a responsabilidade direta pela gestão do conteúdo on-line. Dessa forma, o MCI estabelece um equilíbrio delicado entre a não interferência imediata e a remoção de conteúdos em determinados casos. Quando realizada de maneira adequada, essa abordagem desempenha um papel essencial na preservação de um ambiente digital saudável e seguro, sem comprometer desnecessariamente a liberdade de expressão.

4. MODERAÇÃO DE CONTEÚDO E RESPONSABILIDADE DOS PROVEDORES DE APLICAÇÃO

A liberdade de expressão é um dos pilares da democracia e somente pode ser limitada quando sua prática fere outros direitos fundamentais.

No ambiente digital, os desafios à liberdade de expressão tornam-se ainda mais

33. BRASIL. *Lei nº 12.965, de 23 de abril de 2014: estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil.* Art. 19. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

evidentes, devido à rapidez e à ampla difusão da comunicação on-line. Com o crescimento acelerado do número de usuários da internet, surgem questões complexas sobre os limites do que pode ser publicado e compartilhado, bem como sobre o grau de responsabilidade que as plataformas deveriam assumir na moderação de conteúdo.³⁴

Assim, a busca por um equilíbrio eficaz entre a liberdade de expressão e a moderação por parte das plataformas é um desafio complexo. Um dos principais obstáculos reside na distinção entre o ato ilícito objetivo — facilmente reconhecível e amplamente dado como inaceitável — e o ato ilícito subjetivo, que exige uma análise mais aprofundada e contextualizada para se determinar sua ilicitude.

Ao longo da última década, desde a implementação do Marco Civil da Internet, as práticas de moderação de conteúdo passaram por uma evolução significativa.

Inicialmente, as plataformas adotavam uma abordagem predominantemente reativa, pautando-se nas diretrizes mínimas estabelecidas pelo MCI. Contudo, com o surgimento de novos desafios, esses mecanismos foram aprimorados, levando a sistemas de moderação mais robustos e proativos.

Ou seja, ainda que o MCI normatize apenas a obrigação de retirada de conteúdo pelo provedor de aplicação no caso de nudez ou conteúdo sexual não autorizado e não haja obrigação explícita de supervisão ou monitoramento contínuos, isso não inibiu as plataformas, em resposta às demandas sociais e legais, a criarem regras próprias, chamadas Termos de Serviço, Diretrizes e Políticas de Uso.

Essas diretrizes informam aos usuários quais condutas lhes são exigidas dentro da rede, quais temas e que conteúdos são proibidos e de que forma serão punidos os usuários que desrespeitaram as regras da plataforma. Tudo com o fim de desenvolver um ambiente digital mais seguro, mais sadio e mais propenso ao diálogo civilizado.³⁵

Os Termos de Serviço, Diretrizes e Políticas de Uso são, em verdade, um contrato apresentado pelo qual se exige o consentimento explícito ou tácito do usuário às

34. MONTEIRO, Artur Pericles Lima. *Armadilhas e caminhos da moderação de conteúdo*. Internetlab, 2021. Disponível em: <https://internetlab.org.br/pt/noticias/armadilhas-caminhos-moderacao/>

35. STEIN, Lillian Brandt. *Redes Sociais, Desinformação e Moderação de Conteúdo - 1ª Ed - 2025*. 1. ed. Indaiatuba: Foco, 2024. E-book. Disponível em: <https://plataforma.bvirtual.com.br>.

condições e regras da plataforma sob pena de, em caso de violação, submeter-se às penalidades ali constantes, que passam desde a exclusão da postagem específica ao banimento definitivo da conta na plataforma.³⁶

Como regra, conteúdos evidentemente nocivos à vida, saúde e segurança são excluídos e bloqueados pela maioria dos provedores de aplicação, na tentativa de manter a integridade e a segurança do ambiente on-line.

As plataformas poderiam ter adotado postura mais passiva em relação às suas regras de uso, limitando-se à exclusão somente das postagens de caráter sexual explícito, nos melhores interesses da exigência mínima do MCI. Não parece ter sido assim que se comportou a dinâmica prática evolutiva das redes sociais e das plataformas on-line, todavia.

Na verdade, em resposta aos novos desafios sociais nos confrontos sociais no curso de situações extremas e sem precedentes, como a guerra da Ucrânia ou a pandemia da COVID- 19, entre outros eventos mundiais, as plataformas estão cada vez mais atualizando e aprimorando suas políticas internas para que publicações potencialmente prejudiciais e/ou controversamente agradáveis sejam encontradas, sinalizadas ou até bloqueadas proativamente. De fato, a moderação de conteúdo é uma função complementar e multifacetada,

pois não só propõe diretrizes de uso das plataformas, mas também busca evitar a instalação de um ambiente potencialmente danoso nas redes sociais.³⁷

Seria uma utopia pensar que poderia haver uma rede completamente sem conteúdo ilícito ou ofensivo, pois isso dependeria não apenas de sistemas perfeitos de moderação, mas também da conduta ética e responsável dos próprios usuários.

Com o intuito de realizar a distinção adequada e justa entre o que deve ser removido ou mantido, os provedores de aplicação comumente utilizam critérios predominantemente objetivos, com baixa ambiguidade ou incerteza acerca da ilicitude do conteúdo, abordagem que é particularmente importante uma vez que

36. GOVERNO DIGITAL. Guia para elaboração de termos de uso e políticas de privacidade. Brasília: Governo Federal, 2024. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_termo_uso_politica_privacidade.pdf.

37. STEIN, Lillian Brandt. *Redes Sociais, Desinformação e Moderação de Conteúdo* - 1ª Ed - 2025. 1. ed. Indaiatuba: Foco, 2024. E-book. Disponível em: <https://plataforma.bvirtual.com.br>.

muitos conteúdos são detectados inicialmente por algoritmos da plataforma, que operam em parâmetros de pré-definição e aprendizagem de máquina.

Determinadas palavras-chave ou expressões específicas encontram-se frequentemente banidas em quase todas as plataformas. Elas estão, de modo geral, vinculadas a potenciais delitos ou comportamentos socialmente indesejáveis, tal qual incitação explícita ao cometimento de crimes, ao suicídio, ou o emprego de termos diretamente discriminatórios. Surge, então, o interesse em observar a evolução das práticas de moderação durante o tempo, especialmente em resposta a eventos globais de destaque.

Antes da pandemia da COVID-19, os provedores de aplicação realizavam a prática da moderação do conteúdo duas formas complementares: a moderação humana, para contextos mais complexos, e a moderação algorítmica, para os contextos mais objetivos e que, geralmente, eram claramente percebidos como conteúdos tales ilícitos, como os vídeos de cenas explícitas de violência, ou os textos contendo as palavras-chave sensíveis previamente identificadas.

Entretanto, o cenário global de pós-pandemia gerou mudanças consideráveis neste paradigma, quando houve uma queda do número de moderações realizadas diretamente por humanos, seja devido a razões de segurança dos trabalhadores ou pela demanda de lidar com um maior volume de conteúdo produzido no contexto da paralisação social.

Consequentemente, verificou-se uma preferência crescente pela moderação automatizada, ou seja, aquela realizada prioritariamente por sistemas de inteligência artificial com aprendizado de máquina, em especial este sistema avançado é capaz de aprender com seus próprios erros e acertos e torna-se cada vez mais efetivo e preciso em sua análise subsequente.

Entretanto, é importante ressaltar que estas moderações, principalmente as realizadas com caráter automatizado, não são infalíveis e enfrentam o desafio monumental de lidar com milhões de dados que aparecem em menos de um dia, em várias plataformas on-line; portanto, erros de moderação, tal como a retirada indevida de conteúdo legítimo ou a falha na identificação e retirada de uma postagem

genuinamente ofensiva podem e de fato ocorrem com certa regularidade.³⁸

Um caso notório dessa fragilidade é constatado durante a campanha do Outubro Rosa, quando algumas plataformas, por sua vez, retiraram equivocadamente as fotos educativas dos seios, que visavam trazer informações pertinentes a respeito do câncer de mama, sob a justificativa que as fotos infringiam as diretrizes de usabilidade em relação à nudez.

Esse caso, em particular, é paradigmático da angústia das situações de moderação automatizada, pois a publicação não era de natureza pornográfica nem de nudismo, mas de caráter informativo, tendo os algoritmos das plataformas, em sua lógica binária e sem contexto, categorizado e banido a publicação.

Assim, essa remoção, portanto, poderia ser considerada como o indesejado fenômeno da censura prévia, pois mesmo um conteúdo considerado lícito e educacional estava sendo qualificado como ilícito e removido pelas automatizações. A bem da verdade, episódio evidencia que a moderação automatizada (não obstante estar aprimorada) traz erros, e que se pode errar por excesso ou por omissão.

Não há dúvida de que as plataformas se empenham insistentemente para aprimorar a sua moderação de forma cada vez mais eficaz, com o intuito de promover um ambiente nas redes sociais cada vez mais saudável, seguro e aberto ao diálogo respeitoso. Entretanto, a moderação de conteúdo representa um desafio dinâmico e de grande complexidade, exigindo um equilíbrio cuidadoso para evitar excessos que possam resultar em censura indevida.³⁹

A análise da evolução da moderação de conteúdo evidencia que esse tema continuará a representar um desafio em constante evolução, uma vez que os provedores de aplicação têm intensificado seus investimentos em tecnologias avançadas de inteligência artificial e aprendizado de máquina para aprimorar a precisão da moderação automatizada. Paralelamente, é evidente a importância da supervisão humana e análise específica de cada conteúdo, pois é necessário considerar o contexto da publicação, principalmente em situações de interpretação

38. STEIN, Lílian Brandt. *Redes Sociais, Desinformação e Moderação de Conteúdo - 1ª Ed - 2025*. 1. ed. Indaiatuba: Foco, 2024. E-book. Disponível em: <https://plataforma.bvirtual.com.br>.

39. STEIN, Lílian Brandt. *Redes Sociais, Desinformação e Moderação de Conteúdo - 1ª Ed - 2025*. 1. ed. Indaiatuba: Foco, 2024. E-book. Disponível em: <https://plataforma.bvirtual.com.br>.

subjetiva, como nos casos de verificar se a liberdade de expressão feriu algum dos direitos da personalidade.

5. REANÁLISE DA CONSTITUCIONALIDADE DO ART. 19 DO MARCO CIVIL DA INTERNET PELO SUPREMO TRIBUNAL FEDERAL: JULGAMENTO CONJUNTO DOS TEMAS 987 E 533 DE REPERCUSSÃO GERAL

O aumento do número de usuários nas redes sociais, somado ao incremento na quantidade de ações judiciais relacionadas à irregularidade cometida através das redes sociais, fez com que o Supremo Tribunal Federal (STF) ocupasse um lugar de destaque nesse debate.

Em 2024, a Corte iniciou o julgamento de dois recursos extraordinários que tratam da responsabilidade civil das plataformas de internet por conteúdos de terceiros e a possibilidade dessa remoção de conteúdo sem necessidade de decisão judicial, sendo esses: o RE 1037396 (Tema 987), de relatoria do Ministro Dias Toffoli e o RE 1057258 (Tema 533) de relatoria do Ministro Luiz Fux.⁴⁰

O primeiro recurso discute a constitucionalidade do art. 19 do Marco Civil da Internet, que impõe que a exclusão de conteúdo e a posterior responsabilização civil dos provedores de aplicação só podem ocorrer mediante ordem judicial. O segundo, por sua vez, questiona a obrigação das empresas de fiscalizar o conteúdo publicado e remover material ofensivo, independentemente de uma ordem judicial.

Os temas estão interligados, tendo em vista que ambos versam sobre a responsabilidade das plataformas na remoção de conteúdo sem ordem judicial. Contudo, o Tema 987 merece destaque em razão de discutir a inconstitucionalidade do art. 19 do MCI.

Em seu voto, o Ministro Luiz Fux alegou que o art. 19 do MCI estrutura um ambiente seguro e confortável para os provedores de aplicação e inibe ações proativas para a remoção de conteúdo ilícito. Ademais, defende a posição de que as

40. SUPREMO TRIBUNAL FEDERAL (STF). *STF começa a julgar ações sobre regras do Marco Civil da Internet para remoção de conteúdos*. Brasília, 2024. Disponível em: <https://noticias.stf.jus.br/posts/noticias/stf-comeca-a-julgar-acoes-sobre-regras-do-marco-civil-da-internet-para-remocao-de-conteudos/>.

plataformas devem retirar o conteúdo ilícito assim que notificada. De forma similar, o Ministro Dias Toffoli também votou pela inconstitucionalidade do artigo 19 do MCI, alegando que a notificação extrajudicial seria suficiente para que as plataformas retirassem o conteúdo ilícito.

Além dos relatores, o Ministro Luís Roberto Barroso, presidente do Supremo Tribunal Federal, também expressou seu voto. De maneira distinta dos relatores, o Min. Barroso posicionou-se a favor da parcial inconstitucionalidade do art. 19 da do MCI. O Ministro apresentou uma abordagem mais detalhada: em situações evidentes de violação da lei penal ou à constituição, que requerem, a seu ver, uma análise objetiva da ilicitude, não seria necessária uma decisão judicial prévia, apenas a notificação seria suficiente.

Nos casos de delitos subjetivos, como os crimes contra a honra, as postagens deveriam ser removidas apenas após uma decisão judicial, com essa supervisão pelo Judiciário, sendo esta uma forma de evitar eventual censura prévia. Barroso também se afastou da linha de pensamento dos relatores ao afirmar que a responsabilidade dos provedores de aplicativos deve ser subjetiva, em vez de objetiva, uma vez não há precedentes no direito comparado que sustentem a responsabilidade objetiva dos provedores de aplicação.

Embora apenas três votos tenham sido apresentados até o momento, parece provável que o art. 19 do MCI seja declarado total ou parcialmente inconstitucional. Entre as propostas apresentadas, a do Ministro Barroso aparenta ser a mais equilibrada, pois estabelece critérios mais efetivos para orientar os provedores de aplicação, sem exigir que estes decidam entre direitos fundamentais em casos de ofensas mais subjetivas.

No entanto, alguns pontos da proposta de Barroso merecem uma análise mais aprofundada, como a determinação de que publicações que promovam a abolição violenta do Estado Democrático de Direito ou golpe de Estado também deveriam ser removidas pelas plataformas sem necessidade de decisão judicial.

À medida que o julgamento prossegue, é evidente que a decisão final do STF terá implicações profundas para a regulação da internet no Brasil, potencialmente redefinindo o equilíbrio entre liberdade de expressão, responsabilidade das plataformas e proteção contra conteúdos ilícitos ou ofensivos.

É fundamental considerar as implicações de longo prazo dessa decisão. Uma mudança no regime de responsabilidade das plataformas poderia alterar significativamente a dinâmica da comunicação on-line no Brasil. Isso poderia levar a uma moderação de conteúdo mais rigorosa por parte das plataformas, potencialmente reduzindo a disseminação de conteúdo nocivo, mas também correndo o risco de limitar expressões legítimas.

6. AS POSSÍVEIS IMPLICAÇÕES PARA A LIBERDADE DE EXPRESSÃO EM CASO DE SER DECLARADA INCONSTITUCIONALIDADE DO ART. 19 DO MCI

O iminente proferimento de decisão pelo Supremo Tribunal Federal acerca da constitucionalidade do art. 19 do MCI, suscita profundas reflexões sobre a responsabilidade civil dos provedores de aplicações e como a sua atuação impacta o exercício da liberdade de expressão no ambiente digital.

O MCI, em sua concepção original, pretendeu preservar de maneira veemente o direito à liberdade de expressão, estabelecendo um arcabouço normativo que visa equilibrar o complexo exercício de direitos de diferentes sujeitos que interagem no ecossistema virtual. Enquanto conteúdos explicitamente ilícitos são passíveis de remoção mediante simples notificação, situações de ilicitude menos evidentes são reservadas ao crivo do Judiciário, a fim de preservar o direito à livre manifestação do pensamento, assim como resguardar a atuação do Poder Judiciário em casos que demandam exame de questões evidentemente complexas do ponto de vista jurídico, reconhecendo sua legitimidade precípua na ponderação de direitos fundamentais, como órgão imbuído de jurisdição pela Constituição Federal.

A imposição aos provedores de aplicação do dever de remover indiscriminadamente todo conteúdo apontado como ilícito, mesmo em situações de controvérsia jurídica, pode acarretar uma significativa constrição da liberdade de expressão no meio digital. As plataformas, ante o temor de responsabilização, possivelmente adotarão uma postura de hipercautela, suprimindo conteúdos ao menor indício de violação a direitos, em detrimento do debate público e do

pluralismo de ideias.⁴¹

A imposição aos provedores de aplicação do dever de remover indiscriminadamente todo conteúdo apontado como ilícito, mesmo em situações controvertidas (ou seja, quando não se tem certeza da ilicitude), possivelmente acarretará significativa constrição da liberdade de expressão no meio digital.

As plataformas, ante o temor de responsabilização, possivelmente adotarão uma postura exageradamente cautelosa, suprimindo conteúdos ao menor indício de violação a direitos e suas próprias diretrizes, em detrimento do debate público e do pluralismo de ideias, manifestações concretas do livre exercício da liberdade de expressão.

O papel dos provedores de aplicação deve se limitar à disponibilização da infraestrutura tecnológica para acesso dos usuários e à implementação de mecanismos que promovam um ambiente digital estável e coeso, sem que isso se transmute em uma forma velada de censura prévia. Primordialmente, porque estas entidades não são investidas de jurisdição para arbitrar unilateralmente a legalidade de determinados conteúdos. Secundariamente, porque a liberdade de expressão, como direito fundamental, só pode ser legitimamente restringida quando em colisão com outros direitos de igual hierarquia constitucional, o que deve necessariamente passar pelo devido processo legal.

A discussão sobre a inconstitucionalidade do art. 19 do MCI revela-se um tanto contraditória na medida em que tende a promover a ampliação dos poderes dos provedores de aplicação em detrimento da atuação do Judiciário. Tal abordagem incorre no risco de subverter a função primordial da tutela jurisdicional inerente ao Estado Democrático de Direito, ao transferir para entes privados o poder decisório sobre questões que afetam diretamente direitos fundamentais.⁴²

41. SOUZA, Carlos Affonso de. *As cinco faces da proteção à liberdade de expressão no marco civil da internet*, Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio (ITS Rio), 2018, p. 25. Disponível em: https://itsrio.org/wp-content/uploads/2018/06/as_cinco_faces.pdf.

42. LEMOS, Ronaldo; SOUZA, Carlos Affonso Pereira de; BRANCO, Sergio. Mudar Marco Civil da Internet ameaça liberdade de expressão. *Jornal da Advocacia*, 2023. Disponível em: <https://jornal-daadvocacia.oabsp.org.br/noticias/ponto-de-vista/mudar-marco-civil-da-internet-ameaca-liberdade-de-expressao/>.

Apesar do intuito à proposta de revisão do art. 19 ser o de fomentar uma atuação mais proativa das plataformas na remoção de conteúdos ilícitos, existe um claro risco de que essa abordagem produza consequências não pretendidas e potencialmente deletérias para o ambiente digital⁴³, principalmente pois a transferência do poder decisório do Judiciário para as plataformas digitais, resultará, provavelmente, em um cenário de insegurança jurídica, em prejuízo dos princípios fundamentais, especialmente a liberdade de expressão, que podem não

ser adequadamente tutelados⁴⁴, haja vista que os provedores de aplicação não possuem a expertise necessária para a correta modulação dos limites dos direitos fundamentais.

É necessário reconhecer que a definição do que constitui conteúdo ofensivo é intrinsecamente subjetiva e varia significativamente entre indivíduos e contextos culturais, assim, a resolução dessa problemática deve considerar especialmente a condição da licitude do conteúdo e sua proteção sob o manto da liberdade de expressão.

Não se pode esquecer que os provedores de aplicação têm adaptado suas diretrizes de uso em conformidade com as diretrizes jurisprudenciais e ao contexto mundial que vêm pouco a pouco se consolidando, a fim de fomentar um ambiente on-line mais saudável, porém sem vedar a liberdade de expressão.

A solução ideal para esse problema central, deve ser tratada com muito cuidado, pois é plausível que os provedores de aplicação assumam uma postura mais assertiva em face de fatos constitutivos de ilícitos objetivos, como manifestações explícitas de discurso preconceituoso ou de intolerância religiosa. Contudo, é importante que as plataformas não sejam investidas do dever de remover postagens potencialmente ilícitas que não sejam notoriamente marcadas pela ilicitude, como aquelas

43. LEMOS, Ronaldo; SOUZA, Carlos Affonso Pereira de; BRANCO, Sergio. Mudar Marco Civil da Internet ameaça liberdade de expressão. *Jornal da Advocacia*, 2023. Disponível em: <https://jornal-daadvocacia.oabsp.org.br/noticias/ponto-de-vista/mudar-marco-civil-da-internet-ameaca-liberdade-de-expressao/>.

44. KANAYAMA, Ricardo Alberto. *A liberdade de expressão do Marco Civil da Internet e o procedimento de notificação e retirada para as "infrações" aos direitos autorais*. *Civilística.com*, 2021, p. 21. Disponível em: <https://civilistica.emnuvens.com.br/redc/article/view/495>.

relacionadas à ofensa da honra.

Estas questões, por sua natureza intrinsecamente complexa e contextual, devem permanecer sob a égide do Poder Judiciário, passando pelo crivo do devido processo legal.

Uma abordagem que transfira excessivamente a responsabilidade para as plataformas poderia resultar em uma atividade de moderação excessivamente restritiva e potencialmente arbitrária. Temendo sanções legais, as plataformas poderiam optar por uma política de remoção indiscriminada de conteúdos controversos, efetivamente implementando um regime de censura prévia, em prejuízo do direito fundamental da liberdade de expressão no ambiente digital.

Importante assinalar, ainda, que a simples deliberação pelo Supremo Tribunal Federal pode não ser o suficiente para pacificar uma questão tão complexa e sensível socialmente.

A eventual inconstitucionalidade do art. 19 terá consequências profundas sobre o exercício da liberdade de expressão, seja privilegiando direitos provenientes da dignidade da pessoa humana, seja estimulando um regime de análise prévia pelas plataformas, o que potencialmente gerará supressão de conteúdos com a falta do devido processo legal e do contraditório.

Finalmente, cabe recordar que o MCI é o resultado de um processo legislativo demorado e de extrema complexidade, no qual resultou de um esforço amplo entre e juristas, organizações da sociedade civil e representantes de diversos setores, haja vista a necessidade de um esforço conjunto para compatibilizar a norma em questão com os preceitos constitucionais foram notórios.

A decisão do STF, qualquer que seja, provavelmente transformará significativamente o cenário da internet no Brasil, exigindo uma adaptação cuidadosa por parte de usuários, plataformas e do sistema jurídico como um todo.

7. CONCLUSÃO

Ao longo da última década, o art. 19 do Marco Civil da Internet desempenhou um papel fundamental na regulação do ambiente digital brasileiro, buscando equilibrar a proteção à liberdade de expressão com a necessidade de

responsabilização por conteúdos ilícitos.

Esse dispositivo legal conseguiu, em grande medida, cumprir seu objetivo de salvaguardar a liberdade de expressão ao estabelecer um regime de responsabilidade condicionada para os provedores de aplicação, evitando assim a censura prévia e a remoção indiscriminada de conteúdos.

A eficácia do art. 19 pode ser observada na forma como ele promoveu um ambiente on-line mais aberto e dinâmico, permitindo o florescimento de diversas formas de expressão e debate público. Ao mesmo tempo, ao exigir ordem judicial para a remoção de conteúdos (exceto em casos específicos), o MCI conseguiu coibir o anonimato sem comprometer excessivamente a privacidade dos usuários, criando um mecanismo de responsabilização que respeita o devido processo legal.

Contudo, o cenário digital evoluiu rapidamente, trazendo novos desafios que testaram os limites do modelo estabelecido pelo MCI. A proliferação de desinformação e outros conteúdos potencialmente nocivos levantou questionamentos sobre a adequação do art. 19 frente às demandas contemporâneas de moderação de conteúdo.

A possível declaração de inconstitucionalidade do art. 19 pelo STF tem o potencial de transformar significativamente este cenário. Se por um lado uma mudança poderia permitir uma resposta mais ágil a conteúdos manifestamente ilícitos, por outro, corre-se o risco de abrir caminho para uma forma de censura prévia, com as plataformas possivelmente adotando uma postura excessivamente cautelosa na moderação de conteúdos.

A análise realizada ao longo deste artigo sugere que, embora o art. 19 tenha sido em grande parte bem-sucedido em seu propósito original, o equilíbrio delicado que ele estabelece pode necessitar de ajustes para enfrentar os desafios atuais. No entanto, qualquer alteração deve ser cuidadosamente ponderada, considerando não apenas a eficácia na remoção de conteúdos ilícitos, mas também a preservação do espaço para o livre debate de ideias e a expressão democrática.

Em última análise, o futuro da regulação da internet no Brasil dependerá da capacidade de encontrar um novo equilíbrio que preserve os princípios fundamentais da liberdade de expressão, ao mesmo tempo em que oferece mecanismos eficazes para lidar com os desafios emergentes do ambiente digital. A

decisão do STF, seja qual for, provavelmente marcará o início de uma nova era na governança digital brasileira, exigindo uma adaptação cuidadosa por parte de usuários, plataformas e do sistema jurídico como um todo.

A experiência da última década com o art. 19 do MCI oferece lições valiosas que devem informar este processo de evolução regulatória. O desafio que se apresenta é o de construir sobre as bases estabelecidas pelo MCI, adaptando-as às realidades contemporâneas, sem perder de vista o compromisso fundamental com a liberdade de expressão que tem sido a pedra angular da internet livre e aberta.

REFERÊNCIAS

- ANDRIGHI, Nancy. Marco Civil da Internet. Entrevistada pelo jornal Migalhas, 2013. Disponível em: <https://www.youtube.com/watch?v=-DultHob9Gg&t=52s>.
- BRASIL. Superior Tribunal de Justiça. Recurso Especial 1316921/RJ. Relator: Min. Nancy Andrighi. Julgado em: 26 jun. 2012.
- BRASIL. Lei nº 12.965, de 23 de abril de 2014: estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.
- CÂMARA DOS DEPUTADOS. PL 2126/2011. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=517255>.
- GOVERNO DIGITAL. Guia para elaboração de termos de uso e políticas de privacidade. Brasília: Governo Federal, 2024. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_termo_uso_politica_privacidade.pdf
- KANAYAMA, Ricardo Alberto. A liberdade de expressão do Marco Civil da Internet e o procedimento de notificação e retirada para as "infrações" aos direitos autorais. *Civilística.com*, 2021, p. 21. Disponível em: <https://civilistica.emnuvens.com.br/redc/article/view/495>.
- LEMOS, Ronaldo; SOUZA, Carlos Affonso Pereira de; BRANCO, Sergio. Mudar Marco Civil da Internet ameaça liberdade de expressão. *Jornal da Advocacia*, 2023. Disponível em: <https://jornal-daadvocacia.oabsp.org.br/noticias/ponto-de-vista/mudar-marco-civil-da-internet-ameaca-liberdade-de-expressao/>
- MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. Curso de Direito Constitucional. 12. ed. São Paulo: SaraivaJur, 2017. p. 263.
- MONTEIRO, Artur Pericles Lima. Armadilhas e caminhos da moderação de conteúdo. *Internetlab*, 2021. Disponível em: <https://internetlab.org.br/pt/noticias/armadilhas-caminhos-moderacao/>
- SARMENTO, Daniel. Comentário ao artigo 5º, inciso IV. In: CANOTILHO, J. J. Gomes; MENDES,

Gilmar F.; SARLET, Ingo W.; STRECK, Lenio L. (coord.). Comentários à Constituição do Brasil. São Paulo: Saraiva/Almedina, 2013, p. 255

SENADO FEDERAL. Dez anos de vigência da Lei Carolina Dieckmann: a primeira a punir crimes cibernéticos. 2023. Disponível em: <https://www12.senado.leg.br/radio/1/noticia/2023/03/29/dez-anos-de-vigencia-da-lei-carolina-dieckmann-a-primeira-a-punir-crimes-ciberneticos>.

SOUZA, Carlos Affonso; LEMOS, Ronaldo. Marco Civil da Internet: construção e aplicação. São Paulo: Editora Associada, 2016.

SOUZA, Carlos Affonso Pereira de. As cinco faces da proteção à liberdade de expressão no Marco Civil da Internet. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio (ITS Rio), 2018. Disponível em: https://itsrio.org/wp-content/uploads/2018/06/as_cinco_faces.pdf.

STEIN, Lillian Brandt. Redes Sociais, Desinformação e Moderação de Conteúdo - 1ª Ed - 2025. 1. ed. Indaiatuba: Foco, 2024. E-book. Disponível em: <https://plataforma.bvirtual.com.br>.

SUPREMO TRIBUNAL FEDERAL (STF). STF começa a julgar ações sobre regras do Marco Civil da Internet para remoção de conteúdos. Brasília, 2024. Disponível em: <https://noticias.stf.jus.br/post-noticias/stf-comeca-a-julgar-acoes-sobre-regras-do-marco-civil-da-internet-para-remocao-de-conteudos/>

TEIXEIRA, Tarcisio. Direito Digital e Processo Eletrônico. 7. ed. São Paulo: SaraivaJur, 2023.

UNITED STATES. Communications Decency Act of 1996. S. 314, 104th Congress.

MONITORAMENTO E MODERAÇÃO DE CONTEÚDO MÉDICO NAS REDES SOCIAIS

Gabriella da Silva Reis

Mestra em Direito pela Universidade Federal de Minas Gerais, Especialista em Direito Médico pelo Centro de Ensino Renato Saraiva. Bacharela em Direito pela Universidade Federal do Maranhão. Advogada.

DOI: <https://doi.org/10.59224/dti7.ch12>

Resumo: Este artigo aborda a evolução da publicidade médica frente ao avanço tecnológico e ao uso das redes sociais, destacando a importância do Marco Civil da Internet. Analisa a atuação do CFM e dos CRMs na fiscalização da ética médica online, especialmente após a Resolução CFM 2.336/2023. Examina o papel da Meta na moderação de conteúdo médico no Instagram, utilizando IA para garantir a veracidade das informações. Propõe uma governança colaborativa entre CRMs e plataformas digitais para assegurar um ambiente informativo e ético, enfatizando a necessidade de transparência nas políticas de moderação.

Palavras-chave: Publicidade médica; Monitoramento e Moderação de conteúdo; Governança colaborativa.

Abstract: This article addresses the evolution of medical advertising in the face of technological advancements and the use of social media, highlighting the importance of the Marco Civil da Internet. It analyzes the role of the CFM and the CRMs in overseeing online medical ethics, especially after the implementation of CFM Resolution 2.336/2023. It examines the role of Meta in moderating medical content on Instagram, using AI to ensure the accuracy of information. The article proposes collaborative governance between CRMs and digital platforms to ensure an informative and ethical environment, emphasizing the need for transparency in moderation policies.

Keywords: Medical advertising; Content monitoring and moderation; Collaborative governance.

SUMÁRIO: 1. Introdução; 2. Atuação do Conselho Federal e dos Conselhos Regionais de Medicina; 3. Contexto da Publicidade e Propaganda Médica no Brasil; 4. Monitoramento de conteúdo sobre saúde pelos Conselhos Regionais de Medicina; 5. Moderação de conteúdo de saúde realizado pela Meta no Instagram; 5.1. Marco Civil da Internet e Moderação de Conteúdo; 5.2. Estruturas Organizacionais de Moderação; 5.3. Diretrizes e Políticas da Meta para uso do Instagram; 5.4 Moderação Automatizada; 6. Convergências e Divergências entre o Papel de Monitoramento dos Conselhos Regionais de Medicina e a Moderação de Conteúdo exercida pela Meta; 7. Proposta de Governança Colaborativa; 8. Conclusão; Referências.

1. INTRODUÇÃO

Não por acaso, a publicidade médica sofreu alterações significativas, impactadas por importantes acontecimentos simultâneos: a evolução das telecomunicações, o desenvolvimento tecnológico e científico das ciências da saúde, e o crescimento exponencial dos cursos de medicina. Esse cenário aumentou a concorrência e a necessidade dos novos médicos de se destacarem, nascidos em um ambiente onde a comunicação não se limitava mais às indicações ou aos anúncios impressos, mas ocorria em um ambiente etéreo e virtualizado, com regras difíceis de serem compatibilizadas com a deontologia médica.

Com o advento e a popularização da internet, especialmente das redes sociais, o cenário mudou drasticamente. Plataformas como Instagram, Facebook, “X” (antigo Twitter) e YouTube tornaram-se canais primordiais para a captação de pacientes por médicos e estabelecimentos de saúde, devido à sua acessibilidade e facilidade de uso. Este novo ambiente virtual trouxe consigo desafios únicos, como a necessidade de adaptar as regras de publicidade médica para garantir a ética profissional em um espaço onde a autopromoção e o sensacionalismo são facilmente disseminados.

Paralelamente, a sociedade passou por uma digitalização acelerada, onde a comunicação e a informação se tornaram instantâneas e globais. Este contexto exigiu a criação de novas regulamentações que pudessem assegurar um uso responsável e seguro da internet. É neste cenário que o Marco Civil da Internet foi promulgado em 2014, estabelecendo princípios, garantias, direitos e deveres para o uso da internet no Brasil.

O Marco Civil da Internet trouxe diretrizes fundamentais para a proteção da privacidade dos usuários e a liberdade de expressão, mas também enfatizou a importância da moderação de conteúdo.

Observa-se que a era do marketing de conteúdo, onde informações são publicadas de forma intencional e estratégica para atrair novos pacientes, muitas vezes resulta em práticas enganosas e apelativas. Fotos manipuladas ou, mesmo quando autênticas, apresentadas fora dos preceitos éticos da profissão, violam o Código de Ética Médica e a Resolução CFM 2.336/2023 sobre publicidade médica, além de estarem sujeitas a moderação pelas políticas de conteúdo das plataformas, em observância ao

regime de responsabilidade civil previsto no art. 19 do Marco Civil da Internet.

A transição do meio publicitário físico para o digital impôs novas obrigações aos profissionais de saúde, que agora devem observar outras regras para a veiculação de conteúdo na internet, aquelas ditadas pelo CFM, mas também pelos termos de uso e as políticas de conteúdo nas redes sociais.

Dessa forma, a evolução das regras de publicidade médica reflete não apenas os avanços tecnológicos e a digitalização da sociedade, mas também a necessidade contínua de adaptação e regulamentação para garantir que a prática médica mantenha sua integridade e ética, mesmo em um ambiente virtual dinâmico e desafiador.

O Marco Civil da Internet e as resoluções do CFM apesar de exercerem papéis distintos, com convergências e divergências que serão abordadas ao longo do texto, podem trabalhar em conjunto para assegurar que a publicidade médica na internet seja realizada de maneira responsável, com o objetivo de que os conteúdos sobre saúde sejam informativos, verdadeiros e respeitem a privacidade dos pacientes.

Este artigo, baseado em uma revisão bibliográfica, tem como objetivo debater sobre o papel do CFM e dos CRMs no monitoramento de conteúdo médico publicado em redes sociais e a moderação de conteúdo de saúde realizada pela Meta, no Instagram e Facebook, e como esse tipo de conteúdo é (ou deveria ser) moderado. Ao final, será discutida a possível união de esforços entre autoridades de saúde, visando tornar o monitoramento e a moderação de conteúdo médico mais eficientes, por meio de uma estrutura de governança colaborativa e convênios entre entidades.

2 ATUAÇÃO DO CONSELHO FEDERAL E DOS CONSELHOS REGIONAIS DE MEDICINA

A Lei nº 3.268 de 1957¹ que conferiu o status de autarquia para o Conselho Federal de Medicina (CFM), atribuiu-lhe um papel central na regulamentação e fiscalização da prática médica no Brasil. Esta mesma lei delegou aos Conselhos Regionais de

1. BRASIL. Lei n.º 3.268, de 30 de setembro de 1957. Dispõe sobre os Conselhos de Medicina. Diário Oficial da União: Rio de Janeiro, 30 de set. 1957 Disponível em: https://www.planalto.gov.br/ccivil_03/LEIS/L3268.htm#art36. Acesso em: 24 jun. 2024.

Medicina (CRMs) a responsabilidade de fiscalizar o exercício da profissão médica², apreciar e decidir sobre assuntos relacionados à ética profissional, impondo as penalidades cabíveis. Além disso, os CRMs devem garantir o livre exercício legal dos direitos dos médicos, promover o desempenho técnico e moral da medicina, bem como o prestígio e bom conceito da profissão e de seus praticantes.

É notório que as competências atribuídas aos CRMs são mais voltadas para a vigilância e fiscalização dos médicos do que as do próprio CFM. Embora essa estrutura organizacional vise a uma melhor gestão e fiscalização da profissão, é fundamental destacar essa divisão de atribuições para definir claramente o papel de cada entidade nas discussões subsequentes.

Os CRMs têm a incumbência de receber denúncias sobre atos médicos que constituam infrações ao Código de Ética Médica e possuem a prerrogativa de agir de ofício. As questões levadas aos CRMs não se limitam apenas aos atos médicos ou à relação médico-paciente, mas frequentemente envolvem a conduta observada em entrevistas, campanhas publicitárias e, principalmente, nas redes sociais.

Dentre as atribuições mencionadas, o papel de monitoramento do conteúdo publicado por médicos decorre do dever de promover, por todos os meios ao seu alcance, o perfeito desempenho técnico e moral da medicina e o prestígio e bom conceito da profissão.

Portanto, os conselhos regionais podem agir de ofício³ ao identificar conteúdos que violem os preceitos éticos da profissão, conduzindo sindicâncias quando

-
2. Art. 15. São atribuições dos Conselhos Regionais: c) fiscalizar o exercício da profissão de médico; conhecer, apreciar e decidir os assuntos atinentes à ética profissional, impondo as penalidades que couberem; h) promover, por todos os meios e o seu alcance, o perfeito desempenho técnico e moral da medicina e o prestígio e bom conceito da medicina, da profissão e dos que a exerçam;
 3. Art. 14 A sindicância será instaurada: I – de ofício pelo CRM; II – mediante denúncia escrita ou verbal, na qual conste o relato circunstanciado dos fatos e, quando possível, a qualificação do médico denunciado, com a indicação das provas documentais, além de identificação do denunciante, devendo acompanhar cópias de identidade, CPF, comprovante de endereço, incluindo todos os meios eletrônicos disponíveis para contato. CONSELHO FEDERAL DE MEDICINA (CFM). Resolução CFM nº 2.306/2022. Aprova o Código de Processo Ético-Profissional (CPEP) no âmbito do Conselho Federal de Medicina (CFM) e Conselhos Regionais de Medicina (CRMs). Diário Oficial da União: seção I, Brasília, DF, 25 mar. 2022. Disponível em: https://portal.cfm.org.br/wp-content/uploads/2022/03/2306_2022.pdf. Acesso em 29. jun. 2024.

necessário.

Assim, a atuação dos CRMs se configura como um mecanismo essencial para a manutenção da ética e da integridade na prática médica, especialmente em um contexto onde a exposição e a comunicação pública se tornam cada vez mais frequentes e desafiadoras de serem regulamentadas.

3 CONTEXTO DA PUBLICIDADE E PROPAGANDA MÉDICA NO BRASIL

A publicidade médica é matéria regulada por resolução específica dentro do CFM. Antes estava prevista na Resolução CFM nº 1.974/2011 e foi recentemente revogada pela Resolução CFM 2.336 de 2023⁴.

Conforme o artigo 1º da Resolução nº 2.336/2023 do CFM⁵, a publicidade médica é o ato de promover estruturas físicas, serviços e qualificações do médico ou dos estabelecimentos médicos (físicos ou virtuais) e propaganda é o ato de divulgar assuntos e ações de interesse da medicina.

Historicamente, a regulamentação da publicidade médica no Brasil tem sido guiada pelo princípio de que a medicina não deve ser mercantilizada e que a promoção de serviços deve se manter estritamente informativa, evitando promessas de resultados, sensacionalismo ou qualquer forma de concorrência desleal.⁶

4. CONSELHO FEDERAL DE MEDICINA (CFM). Resolução CFM nº 2.336/2023. Dispõe sobre publicidade e propaganda médicas. Diário Oficial da União: seção I, Brasília, DF, 13 set. 2023. Disponível em: <https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2023/2336>. Acesso em 08. jun. 2024.

5. Ibid. Art. 1º Para fins desta Resolução, entende-se por publicidade ou propaganda médica a comunicação ao público, por qualquer meio de divulgação da atividade profissional, com iniciativa, participação e/ou anuência do médico, nos segmentos público, privado e filantrópico. §1º Entende-se por publicidade médica o ato de promover estruturas físicas, serviços e qualificações do médico ou dos estabelecimentos médicos (físicos ou virtuais). §2º Entende-se por propaganda médica o ato de divulgar assuntos e ações de interesse da medicina.

6. Capítulo XIII É vedado ao médico: Art. 111. Permitir que sua participação na divulgação de assuntos médicos, em qualquer meio de comunicação de massa, deixe de ter caráter exclusivamente de esclarecimento e educação da sociedade. Art. 112. Divulgar informação sobre assunto médico de forma sensacionalista, promocional ou de conteúdo inverídico. CONSELHO FEDERAL DE MEDICINA (CFM). Resolução nº 2.217/2018. Código de Ética Médica. Diário Oficial da União:

A Resolução CFM 2.336/2023 trouxe maior clareza sobre o que constitui conduta ética nas redes sociais e concedeu mais liberdade para a produção de conteúdo de saúde. Entre as principais inovações trazidas pela Resolução nº 2.336/2023, destacam-se a ênfase na transparência e na veracidade das informações divulgadas. A resolução proíbe expressamente o uso de imagens que possam criar expectativas não realistas sobre os resultados dos tratamentos, bem como a promoção de técnicas inovadoras sem o devido respaldo científico.

Outro ponto de destaque é a adaptação às novas mídias e plataformas digitais. Com a popularização das redes sociais e dos sites especializados em saúde, tornou-se imperativo que as normas de publicidade médica contemplassem esses novos canais de comunicação. A Resolução nº 2.336/2023 aborda essa questão ao estabelecer diretrizes específicas para a publicidade em ambientes digitais, garantindo que a divulgação de serviços médicos nesses espaços respeite os mesmos princípios éticos aplicados aos meios tradicionais de comunicação⁷.

Além disso, há previsão expressa de que os conselhos regionais devem manter uma Comissão de Assuntos Médicos (Codame)⁸. As comissões têm, além do papel de fiscalizar a publicidade e propaganda médica, a incumbência de elaborar campanhas educativas em âmbito nacional e local, com o objetivo de esclarecer a aplicação das regras estabelecidas por esta Resolução.

Destaca-se ainda a responsabilidade de convocar médicos e suas empresas para receberem orientações adequadas quando estiverem divulgando a profissão em

Brasília, DF, 2019. Disponível em: <https://portal.cfm.org.br/images/PDF/cem2019.pdf>. Acesso em: 24 jun. 2024.

7. DANTAS, Eduardo. *Breves Apontamentos sobre a Publicidade e Propaganda na Atividade Médica em Seus Aspectos Éticos e Deontológicos*. A Nova Resolução CFM Nº 2.336/2023. Centro de Investigação de Direito Privado (CIDP). Artigo da Revista Jurídica Luso-Brasileira, v. 01, p. 139-188, 2024. Disponível em: https://www.cidp.pt/revistas/rjlb/2024/1/2024_01_0139_0188.pdf. Acesso em: 24 jun. 2024.

8. Art. 15. Os CRMs devem manter, conforme seus Regimentos Internos, uma Comissão de Divulgação de Assuntos Médicos (Codame), composta, minimamente, por três membros. CONSELHO FEDERAL DE MEDICINA (CFM). Resolução CFM nº 2.336/2023. Dispõe sobre publicidade e propaganda médicas. Diário Oficial da União: seção I, Brasília, DF, 13 set. 2023. Disponível em: <https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2023/2336>. Acesso em 08. jun. 2024.

desacordo com as normas vigentes. Essas ações visam não apenas assegurar o cumprimento das diretrizes, mas também promover uma compreensão ampla e correta sobre a ética na publicidade médica.

Esta evolução da normativa do CFM, ainda que possa ser considerada como tardia, encontra correspondência com a evolução das leis nacionais, uma vez que o contexto de avanço tecnológico e novos desdobramentos que surgem da internet impulsionaram o surgimento de leis como o Marco Civil da Internet que completa 10 anos em 2024.

A nova resolução sobre publicidade médica não apenas responde às exigências de um contexto médico em evolução, mas também se propõe a liderar uma transformação na cultura de comunicação na saúde. Este aspecto é particularmente relevante em uma era definida pela informação rápida e pelo consumo de conteúdo digital, onde a distinção entre informação e publicidade pode se tornar turva.

Um dos pontos mais sensíveis antes da publicação desta resolução era a proibição do uso de imagens de "antes e depois". As fotografias de "antes e depois" têm sido amplamente utilizadas na publicidade médica, especialmente em campos como a dermatologia e a cirurgia plástica, como uma forma de ilustrar os potenciais resultados de tratamentos.

Enquanto tais imagens podem servir como uma ferramenta informativa, elas também correm o risco de criar expectativas irreais ou enganosas. O problema surge quando essas imagens são manipuladas, selecionadas de forma enviesada ou apresentadas sem um contexto adequado, podendo levar os pacientes a ter expectativas não realistas sobre os resultados que podem ser alcançados⁹.

Médicos que realizam procedimentos estéticos, como cirurgias plásticas e dermatologistas, frequentemente se opunham a essa proibição, alegando que precisavam demonstrar seu trabalho através dos resultados obtidos. Os conselhos, por sua vez, argumentavam que a proibição visava evitar a promessa de resultados, já que o resultado estético alcançado por um paciente pode não ser o mesmo para outro,

9. SIMPLÍCIO, A. H. *Social media and Dentistry: ethical and legal aspects*. Dental Press Journal of Orthodontics, v. 24, n. 6, p. 80-89, dez. 2019. DOI: 10.1590/2177-6709.24.6.080-089.sar. Disponível em: https://www.scielo.br/scielo.php?script=sci_art-text&pid=S217694512019000600080&lng=en&nrm=iso&tlng=en. Acesso em: 01 jun. 2024.

gerando falsas expectativas¹⁰.

Essa questão também era frequentemente judicializada, resultando em ações indenizatórias por danos morais ou estéticos devido à frustração de pacientes com os resultados de procedimentos como abdominoplastias e rinoplastias. Doutrina e jurisprudência têm estabelecido que, com exceção de procedimentos estéticos, a atividade médica é de meio, não de resultado.¹¹

A controvérsia também era debatida no judiciário. Um caso de grande repercussão foi a decisão do Tribunal Regional Federal da 1ª Região, que anulou dispositivo da Resolução CFM nº 1.974/2011, permitindo a exposição da figura do paciente pelo médico com autorização expressa do paciente. A decisão¹² autorizou uma cirurgia plástica a divulgar seu trabalho na internet sem sofrer penalidades do seu conselho de classe.

O juiz Anderson Santos da Silva entendeu que a resolução violava a reserva legal para o exercício de qualquer trabalho, ofício ou profissão, lembrando que a Constituição adota o princípio da liberdade para o exercício de qualquer trabalho, desde que qualquer restrição seja expressamente prevista em lei. A decisão fragilizou os argumentos do CFM, CRMs e sociedades de especialidades, que naquela data proibiam expressamente a prática de "antes e depois", na vigência da Resolução CFM

10. CONSELHO REGIONAL DE MEDICINA DO PARANÁ (CRM-PR). Antes e depois: por que não pode. Disponível em: <https://www.crmpr.org.br/Antes-e-depois-por-que-nao-pode-13-51491.shtml>. Acesso em: 24 jun. 2024.

11. De acordo com vasta doutrina e jurisprudência, a cirurgia plástica estética é obrigação de resultado, uma vez que o objetivo do paciente é justamente melhorar sua aparência, comprometendo-se o cirurgião a proporcionar-lhe o resultado pretendido. No caso vertente, verifica-se que o Tribunal de origem arbitra o quantum indenizatório em R\$ 50.000,00 (cinquenta mil reais), pelos danos morais que a recorrida experimentou em decorrência do erro médico produzido pelo recorrente, que além de ter contrariado as expectativas da paciente com os resultados alcançados na cirurgia íntima de natureza estética a que foi submetida, gerou-lhe prejuízos em sua saúde. 5. Agravo regimental não provido. (STJ - AgRg nos EDcl no AREsp: 328110 RS 2013/0110013-4, Relator: Ministro LUIS FELIPE SALOMÃO, Data de Julgamento: 19/09/2013, T4 - QUARTA TURMA, Data de Publicação: DJe 25/09/2013)

12. VALOR. *Justiça autoriza propaganda com antes e depois de pacientes*. Disponível em: <https://valor.globo.com/patrocinado/dino/noticia/2022/12/07/justica-autoriza-propaganda-com-antes-e-depois-de-pacientes-1.ghtml>. Acesso em: 29 jun. 2024.

1.974/2011.

A polêmica foi parcialmente desfeita com a autorização dada pelo art. 14 da nova resolução que autorizou a divulgação de imagens de "antes e depois", exigindo a apresentação de casos semelhantes, explicação sobre o caso clínico, recomendações e possíveis efeitos adversos¹³.

O Manual da Codame¹⁴ tem explicações didáticas de como o médico pode postar conteúdo no formato antes e depois, orientando, conforme exigido no art. 14, alínea "b" da Resolução CFM 2.336/2023 que as fotos devem ser apresentadas em um conjunto de imagens contendo indicações, evoluções satisfatórias, insatisfatórias e complicações decorrentes da intervenção, sendo vedada a demonstração e ensino de técnicas que devem limitar-se ao ambiente médico.

Tal medida se impõe, pois, a publicidade persuasiva nas redes sociais transmitidas por fotografias atraentes pode ter consequências negativas não intencionais para a imagem corporal e a autoestima de alguns usuários, criando expectativas irrealistas de tratamento¹⁵. O público geralmente desconhece que os profissionais exibem resultados bem-sucedidos de forma seletiva, e que essas imagens podem não refletir as verdadeiras habilidades e proficiência do profissional.

13. RESOLUÇÃO CFM Nº 2.336/2023. Art. 14, "II– a demonstração de resultados de técnicas e procedimentos, respeitados os seguintes princípios: a) qualquer uso de imagem deve ser acompanhado de texto educativo contendo as indicações terapêuticas, fatores que influenciam possíveis resultados e descrição das complicações descritas em literatura científica; b) demonstrações de antes e depois devem ser apresentadas em um conjunto de imagens contendo indicações, evoluções satisfatórias, insatisfatórias e complicações decorrentes da intervenção, sendo vedada a demonstração e ensino de técnicas que devem limitar-se ao ambiente médico; c) quando aplicável, apresentar evolução para diferentes biotipos e faixas etárias, bem como evoluções imediatas, mediatas e tardias das intervenções demonstradas;
14. CONSELHO REGIONAL DE MEDICINA DO MARANHÃO (CRM-MA). Manual de Publicidade. Disponível em: <https://crmma.org.br/wp-content/uploads/2024/03/Manual-de-publicidade-completo-1.pdf>. Acesso em: 30 jun. 2024.
15. SIMPLÍCIO, A. H. *Social media and Dentistry: ethical and legal aspects*. Dental Press Journal of Orthodontics, v. 24, n. 6, p. 80-89, dez. 2019. DOI: 10.1590/2177-6709.24.6.080-089.sar. Disponível em: https://www.scielo.br/scielo.php?script=sci_art-text&pid=S217694512019000600080&lng=en&nrm=iso&tlng=en. Acesso em: 01 jun. 2024.

A regulação¹⁶ da publicidade médica busca equilibrar o direito à informação do público com a necessidade de preservar a ética e a dignidade da profissão médica, evitando práticas que possam induzir a erro ou criar falsas expectativas nos pacientes. Assim, a publicidade médica deve ser exercida com responsabilidade e rigor ético, em conformidade com as diretrizes estabelecidas pelos órgãos competentes.

É importante notar que, embora a publicidade em sentido amplo seja um direito consagrado pela Constituição Federal, seu exercício não é ilimitado. O Conselho Nacional de Autorregulamentação Publicitária (CONAR) desempenha um papel de destaque ao fiscalizar a licitude do material divulgado, assegurando que a publicidade respeite as normas vigentes.

Além disso, no contexto da publicidade médica, devido à natureza consumerista dessa relação, a divulgação de material com conteúdo enganoso ou abusivo pode acarretar responsabilidade civil para o profissional de saúde. Essa responsabilidade decorre não apenas das normas éticas estabelecidas pelo CFM, mas também das disposições legais que visam proteger o consumidor, garantindo a veracidade e a integridade das informações divulgadas.

Conforme será exposto ao longo do texto, o conteúdo publicado por médicos também está sujeito à moderação realizada pelas plataformas, como a Meta, subordinadas aos preceitos do Marco Civil da Internet para promoção do uso seguro, consciente e responsável da internet.

A implementação efetiva da resolução requer um esforço conjunto de todos os envolvidos no setor de saúde, incluindo os próprios médicos, as instituições de saúde, as associações profissionais e os órgãos reguladores. Para tal, o CFM prevê

16. Outro aspecto importante é a diferenciação entre regulação e regulamentação no direito brasileiro, compreendendo-se a regulação no âmbito jurídico como “conjunto de regras de conduta e de controle da atividade econômica pública e privada e das atividades sociais não exclusivas do Estado, com a finalidade de proteger o interesse público”, traduzindo a intervenção do Estado nas atividades econômicas, enquanto que por regulamentação, extrai-se o exercício do poder regulamentar, ato privativo do chefe do Poder Executivo, que se destina a complementar a lei para que se torne mais operativa e funcional sem provocar inovação no ordenamento jurídico (DI PIETRO, 2003, p. 30) Apud. DANTAS, Juliana de Oliveira Jota; MOTA NETO, Leonardo Lima. *Liberdade de Expressão versus Responsabilidade dos Provedores no Marco Civil da Internet*. Revista da AGU, Brasília, v. 21, n.º 04, p. 143-162, out./dez. 2022.

mecanismos de fiscalização e monitoramento, além de estabelecer canais de denúncia para que infrações às diretrizes sejam adequadamente investigadas e sancionadas. Essa estrutura de governança¹⁷ demonstra um compromisso com a aplicação prática das normas estabelecidas, essencial para a sua eficácia.

Esta contextualização foi necessária para atualizar o leitor sobre o cenário e principais polêmicas sobre o tema de conteúdo médico nas redes sociais. Nas próximas seções, discutiremos o papel do CFM e dos CRMs no monitoramento do conteúdo publicado por médicos nas redes sociais, explorando não somente a função fiscalizadora e punitiva dos conselhos regionais, mas também como essas entidades podem colaborar na preservação do conteúdo de saúde publicado por médicos.

4 MONITORAMENTO DE CONTEÚDO SOBRE SAÚDE PELOS CONSELHOS REGIONAIS DE MEDICINA

Os CRMs podem exercer o papel de monitoramento do conteúdo publicado por médicos nas redes sociais, e o fazem através das Codames, que após a publicação da Resolução CFM 2.336/2023 receberam atribuem específica de convocar médico para esclarecer sobre potencial descumprimento de normas contidas na Resolução e orientar a imediata suspensão do anúncio, sem prejuízo de outras medidas.¹⁸

Constata-se, portanto, que após a atualização de suas diretrizes sobre publicidade e propaganda, o CFM adotou uma postura mais moderada em relação à penalização de médicos pelos conteúdos que publicam, optando por um procedimento de notificação e convocação com caráter educacional.

17. COMITÊ GESTOR DA INTERNET NO BRASIL. *Princípios para a Governança e Uso da Internet no Brasil*. Disponível em: <https://principios.cgi.br/>. Acesso em: 8 jun. 2024.

18. Art. 16, III – convocar médico e Diretor Técnico - Médico, quando se tratar de pessoa jurídica, para esclarecer sobre potencial descumprimento de normas contidas nesta Resolução e seu Manual, orientando a imediata suspensão do anúncio e, para dar validade, registrar em ata as orientações, que será assinada por membro da Codame e o interessado (médico, quando pessoa física, e Diretor Técnico – Médico ou preposto médico devidamente identificado e autorizado, quando pessoa jurídica), sem prejuízo de outras medidas; CONSELHO FEDERAL DE MEDICINA (CFM). Resolução CFM nº 2.336/2023. Dispõe sobre publicidade e propaganda médicas. Diário Oficial da União: seção I, Brasília, DF, 13 set. 2023. Disponível em: <https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2023/2336>. Acesso em 08. jun. 2024.

Essa atuação revela que, neste momento pós-publicação da resolução, o poder de fiscalização foi transformado em monitoramento. O objetivo do monitoramento de conteúdo é promover o desempenho técnico e moral da medicina, sem que necessariamente resulte em sanções disciplinares.

Além disso, associações de médicos especialistas, como a Sociedade Brasileira de Cirurgia Plástica (SBCP), também exercem poder de monitoramento sobre seus membros, podendo notificar e punir independentemente da atuação do CRM e Codame.

Um exemplo dessa atuação ocorreu em 2022, quando a SBCP¹⁹ publicou nota com sanções disciplinares a 10 médicos, incluindo suspensões e exclusões, por uso indevido de imagens de pacientes, quebra de decoro, sensacionalismo e autopromoção. As penalidades aplicadas pela SBCP incluem advertência sigilosa, advertência pública, suspensão e expulsão, demonstrando um procedimento rigoroso de fiscalização e punição.

Durante a Pandemia de COVID-19, entidades como a OMS, ANVISA e os conselhos profissionais de saúde adotaram uma postura ativa nas redes sociais com três objetivos principais: orientar, divulgar notícias verídicas e monitorar conteúdos falsos. Apesar desses esforços, surgiram várias manifestações de grupos médicos em redes sociais defendendo pautas como “tratamento precoce” e “kit covid”, que posteriormente foram objeto de responsabilização pelo Poder Judiciário.

As consequências de publicação de conteúdo não verificado podem ser encontradas em decisões como a da Justiça Federal no Rio Grande do Sul que condenou os responsáveis pela publicação do material publicitário intitulado Manifesto Pela Vida, que estimulava o consumo de medicamentos para um suposto “tratamento precoce”. Nas sentenças, a organização Médicos Pela Vida e empresas associadas foram condenadas ao pagamento de R\$ 55 milhões por danos morais coletivos e à saúde.²⁰

19. ESTADO DE MINAS. *SBCP suspende e exclui médicos por conduta nas redes: especialista explica*. Disponível em: https://www.em.com.br/app/noticia/bem-viver/2022/02/25/interna_bem_viver,1348304/sbcp-suspende-e-exclui-medicos-por-conduta-nas-redes-especialista-explica.shtml. Acesso em: 24 jun. 2024.

20. CNN BRASIL. *Justiça condena defensores de tratamento precoce contra covid a pagar R\$ 55 milhões*. Disponível em: <https://www.cnnbrasil.com.br/saude/justica-condena-defensores-de->

No mesmo contexto, médicos dos Estados Unidos, que promoveram a hidroxicloroquina como “cura para a Covid-19” e desestimularam o uso de máscaras também enfrentaram repercussões, com remoção de conteúdo pelas plataformas Facebook, YouTube e Twitter por disseminação de desinformação.²¹

Mesmo com a entrada em vigor da Resolução CFM 2.336/2024 em março de 2024, e a adoção de uma postura de monitoramento e educação pelos CRMs, é importante destacar que as publicações de médicos continuam sujeitas ao poder sancionador do conselho. A atuação dos CRMs mantém seu caráter disciplinar, regido pelo Código de Processo Ético-Profissional – Resolução CFM Nº 2.306/2022. De acordo com o artigo 14, I dessa resolução, os conselhos podem agir de ofício, notificando seus inscritos conforme a respectiva jurisdição.

Podendo agir de ofício a partir da visita às redes sociais de seus inscritos, o procedimento posterior à constatação de infração ética cometida em publicidade ou propaganda médica deve seguir o rito previsto na Resolução CFM Nº 2.306/2022. A sindicância, que é o processo de investigação, pode ser instaurada de ofício pelo CRM ou mediante denúncia escrita ou verbal. A denúncia deve incluir um relato detalhado dos fatos, a identificação do médico denunciado e provas documentais, além da identificação do denunciante com cópias de identidade, CPF e comprovante de endereço.

Durante a fase de sindicância, não são garantidos o contraditório e a ampla defesa. Havendo elementos suficientes, o conselheiro pode elaborar o relatório conclusivo de imediato, que será levado à Câmara de Sindicância para apreciação. Facultativamente, é admitida a manifestação preliminar escrita do denunciado, a requisição de prontuário e outros documentos necessários à verificação dos indícios de autoria e materialidade da infração ética.

O relatório conclusivo indicará a existência ou inexistência de indícios de infração ao Código de Ética Médica. A Câmara de Sindicância pode propor conciliação, termo de ajustamento de conduta (TAC), arquivamento ou instauração de processo ético-profissional (PEP). Tanto a sindicância quanto o processo ético-profissional

tratamento-precoce-contr-a-covid-a-pagar-r-55-milhoes/. Acesso em: 24 jun. 2024.

21. EXAME. *Médicos em vídeo banido nos EUA já negaram gravidade do coronavírus*. Disponível em: <https://exame.com/mundo/medicos-em-video-banido-nos-eua-ja-negaram-gravidade-do-coronavirus/>. Acesso em: 24 jun. 2024.

tramitam em sigilo, dificultando a localização de casos concretos para exemplificar a atuação do conselho nesta matéria.

Os CRMs têm a responsabilidade de garantir que os conteúdos publicados por médicos nas redes sociais sejam verdadeiros e éticos, protegendo tanto os profissionais de saúde quanto os pacientes. O papel dos Conselhos Regionais de Medicina vai além do poder de polícia, envolvendo um monitoramento ético dos comportamentos de seus inscritos nas redes sociais para preservar a integridade da profissão e proteger os pacientes de conteúdos manipulados e enganosos.

Considerando que os conteúdos publicados por médicos estão sujeitos não só às normas do Código de Ética Médica e Resolução 2.336/2023, mas também ao Marco Civil da Internet e aos termos de uso das plataformas, é necessário analisar a moderação de conteúdo de saúde realizada pela Meta, no Instagram, no próximo tópico.

5 MODERAÇÃO DE CONTEÚDO DE SAÚDE REALIZADO PELA META NO INSTAGRAM

Este capítulo examinará como a Meta, através do Instagram, modera o conteúdo de saúde publicado por médicos, utilizando o Marco Civil da Internet como base regulatória. Discutiremos as estruturas organizacionais de moderação, as diretrizes específicas da Meta, como as políticas de publicidade de saúde e as Diretrizes da Comunidade, e a aplicação de inteligência artificial na identificação e gestão de conteúdo. Além disso, serão abordadas as complexidades e desafios da moderação, especialmente no que tange à transparência das políticas e à colaboração necessária entre plataformas digitais e autoridades de saúde.

5.1 Marco Civil da Internet e Moderação de Conteúdo

A Lei nº 12.965 de 2014, conhecida como Marco Civil da Internet (MCI)²², estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. O MCI assegura a liberdade de expressão e proíbe a censura prévia, promovendo um

22. BRASIL. Lei n.º 12.965, de 23 de abril de 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 24 jun. 2024.

ambiente onde os usuários podem compartilhar informações e opiniões livremente, desde que respeitem os direitos dos outros.

Esses objetivos do MCI são diretamente aplicáveis à moderação de conteúdo publicado por médicos em redes sociais. A responsabilidade dos provedores em moderar conteúdos conforme diretrizes claras e a promoção de um ambiente seguro e inovador são essenciais para manter a integridade e a confiança nas informações compartilhadas sobre cuidados de saúde.

No contexto da moderação de conteúdo nas plataformas digitais, o MCI permite que provedores estabeleçam critérios de moderação e remoção de conteúdo por meio de políticas de uso. O MCI busca prevenir abusos e filtrações injustificadas, garantindo o contraditório e a ampla defesa.

A responsabilidade civil dos provedores de aplicação no MCI está centrada na ideia de que os provedores não devem ser responsabilizados pelos conteúdos gerados por terceiros, exceto se, após ordem judicial específica, não removerem o conteúdo ilícito²³.

5.2 Estruturas Organizacionais de Moderação

Chuyi Sheng²⁴ classifica redes sociais como provedores de aplicação de internet, que disponibilizam conteúdos e serviços aos usuários por meio de plataformas online. Segundo o autor, as redes sociais adotam diferentes estruturas organizacionais para a moderação de conteúdo.

Algumas plataformas, como Facebook e YouTube, utilizam a moderação centralizada, onde políticas gerais são aplicadas globalmente. Outras, como Reddit, seguem um modelo descentralizado, permitindo que múltiplos moderadores estabeleçam regras específicas para diferentes subcomunidades.

Na divisão feita por Chuyi Sheng, a moderação de conteúdo pode ocorrer antes

23. BREGA, Gabriel Ribeiro. *A Regulação de conteúdo nas redes sociais: uma breve análise comparativa entre o NetzDG e a solução brasileira*. Revista Direito GV. São Paulo: Direito GV, v. 19, n. 44, p. 01-27, mar. 2023.

24. SHENG, Chuyi. *Automated Content Moderation*. Georgetown Law Technology Review. Washington: Georgetown Law School. v. 06, n. 01, p. 351-363, Jun. 2022.

ou depois da publicação. A ex-ante moderação, frequentemente automatizada, verifica o conteúdo antes de ser publicado. Já a ex-post moderação envolve a remoção de conteúdo após sua publicação, podendo ser reativa (após denúncia) ou proativa (busca ativa por conteúdo inadequado).

A transparência das regras de moderação é fundamental para garantir a confiança dos usuários. As plataformas que divulgam claramente suas políticas de conteúdo, permitem maior compreensão e conformidade por parte dos usuários. A falta de transparência, por outro lado, pode gerar desconfiança e controvérsias.

Por sua vez, Kenneth A. Bamberger e Deirdre K. Mulligan²⁵, propõem um modelo funcional para a moderação de conteúdo, destacando a necessidade de uma abordagem estruturada e distribuída para garantir a governança legítima dos sistemas de moderação de conteúdo.

Os autores afirmam que "*a moderação de conteúdo não é uma função única e diferenciada. É composta por uma variedade de subfunções—tarefas e decisões individuais que podem ser 'delegadas' a diferentes atores humanos e técnicos para serem realizadas de maneiras diferentes, com diferentes implicações normativas e políticas.*"

A Meta, tem regras esparsas e pouco transparentes quanto à moderação de conteúdo. É possível encontrar parâmetros do que é proibido e o que passa por moderação nos Termos de Serviço da Meta, os Termos de Uso do Instagram, Política de Publicidade da Meta para saúde e bem-estar, Diretrizes da Comunidade (Instagram), além de informação dispersas em sua Central de Transparência.

5.3 Diretrizes e Políticas da Meta para uso do Instagram

Para assegurar a veracidade e a integridade das informações de saúde divulgadas no Instagram, a Meta implementa diretrizes espalhadas em vários documentos. Por isso foi realizada a revisão dos principais documentos destacando entre eles a Diretrizes da Comunidade (Instagram), Política de Publicidade da Meta para saúde e bem-estar.

25. MULLIGAN, Deirdre, K.; BAMBERGER, Kenneth A. *Allocating Responsibility in Content Moderation: A Functional Framework*. Berkeley Technology Law Journal. Berkeley: University of California School of Law. v. 36, n. 03, p. 1091-1171, 2021.

No Instagram, as Diretrizes da Comunidade²⁶ têm regras específicas sobre nudez, um tipo de conteúdo que acaba sendo utilizado por médicos, principalmente cirurgiões plásticos. A plataforma não permite nudez em fotos, vídeos ou conteúdos digitais que mostrem relações sexuais, genitais ou nádegas totalmente expostas. No entanto, são abertas exceções para imagens no contexto de amamentação, parto, situações relacionadas à saúde, como pós-mastectomia, conscientização sobre câncer de mama ou cirurgia de confirmação de gênero, além de protestos. Nudez em obras de arte, como pinturas e esculturas, também é permitida.

A Política de Publicidade da Meta para saúde e bem-estar²⁷ destaca-se a proibição de alegações de saúde não realistas. Isso inclui, por exemplo, alegações falsas sobre o tratamento de doenças, como curar, melhorar ou eliminar doenças incuráveis ou terminais sem comprovação científica. Além disso, qualquer promoção de consequências ou resultados específicos deve obrigatoriamente mencionar qualificações ou avisos legais adequados. A utilização de táticas de isca de engajamento, que empregam linguagem sensacionalista ou outras estratégias para atrair engajamento de forma desonesta, também é terminantemente proibida.

Durante a Pandemia de COVID-19, diversas situações exemplificaram a aplicação dessas políticas. O Comitê de Supervisão da Meta confirmou a decisão do Facebook de manter uma postagem de um conselho médico estadual que afirmava que os lockdowns seriam ineficazes para o enfrentamento da pandemia e que teriam sido condenados pela Organização Mundial da Saúde. Embora o conteúdo contivesse informações imprecisas, o Comitê considerou que ele não representava um risco iminente e que a remoção não seria a melhor solução para combater a desinformação.²⁸

Outra controvérsia envolveu o uso medicinal da ayahuasca, uma bebida psicoativa utilizada em algumas religiões brasileiras. O Comitê de Supervisão considerou que a postagem não violava as diretrizes da comunidade do Instagram e recomendou

26. INSTAGRAM. *Ajuda: Community Guidelines*. Disponível em: https://help.instagram.com/477434105621119?ref=igtos&helpref=faq_content. Acesso em: 24 jun. 2024.

27. FACEBOOK BUSINESS. *Ajuda: Políticas de Publicidade*. Disponível em: <https://pt-br.facebook.com/business/help/248923537779939?id=434838534925385>. Acesso em: 24 jun. 2024.

28. INSPER. *Como funciona a Suprema Corte da moderação da Meta*. Disponível em: <https://www.insper.edu.br/noticias/como-funciona-a-suprema-corte-da-moderacao-da-meta/>.

Acesso em: 24 jun. 2024.

que a Meta revisasse suas regras para permitir a discussão sobre o uso tradicional ou religioso de drogas não medicinais de maneira positiva.²⁹

Além disso, em um caso relacionado à conscientização sobre o câncer de mama, o Comitê de Supervisão se posicionou contra a remoção de uma postagem no Instagram. A postagem havia sido removida devido à política de nudez, mas o Comitê considerou que a exceção para "conscientização sobre o câncer de mama" deveria ser aplicada e expressou preocupação com a moderação automatizada de conteúdos relacionados a direitos humanos.³⁰

A falta de transparência nas políticas de moderação do Instagram compromete a eficácia da governança colaborativa de conteúdo. Usuários frequentemente desconhecem os limites de sua expressão sobre conteúdos de saúde até que seus posts sejam removidos ou suas contas penalizadas. Para um gerenciamento mais efetivo, é imprescindível que as autoridades de saúde colaborem com as plataformas, fornecendo orientações claras sobre conteúdos que carecem de reconhecimento científico ou que violam normas éticas. A construção de políticas de moderação mais transparentes é fundamental para assegurar a veracidade e a integridade das informações de saúde divulgadas.

5.4 Moderação Automatizada

As redes sociais utilizam diferentes modelos para decidir sobre a remoção de conteúdo: moderação manual, realizada por humanos; moderação automatizada, executada por algoritmos; e moderação híbrida, que combina algoritmos e intervenção humana. A maioria das plataformas adota o modelo híbrido, onde algoritmos identificam conteúdos problemáticos para revisão humana.

Existem duas abordagens principais para a moderação automatizada³¹: *matching* (correspondência) e *prediction* (predição). No *matching*, métodos como o *hashing* transformam conteúdos em cadeias de dados, permitindo comparações rápidas com

29. Ibid.

30. Ibid.

31. SHENG, Chuyi. *Automated Content Moderation*. Georgetown Law Technology Review, v. 06, n. 01, p. 351-363, Jun. 2022, p. 355.

uma base de dados de conteúdo indesejados. O *hashing* perceptivo foca nas características específicas do conteúdo para identificar similaridades. Na predição, o processamento de linguagem natural e redes neurais analisam e classificam textos, convertendo palavras em valores numéricos e criando regras internas para identificar novos exemplos. Imagens e vídeos são analisados com base em formas, texturas e cores.

Essas técnicas oferecem benefícios como rapidez, eficiência, menor dependência de moderação humana e custos reduzidos. Contudo, erros na moderação podem afetar muitos usuários, e a falta de transparência sobre o funcionamento dessas ferramentas, aliada à ausência de regulamentação específica, aumenta a vulnerabilidade dos usuários.

O Instagram utiliza inteligência artificial (IA) e analistas humanos para identificar, analisar e gerenciar conteúdos que possam violar suas Diretrizes da Comunidade³². As diretrizes definem o que é e não é permitido na plataforma, aplicando-se globalmente com o objetivo de incentivar a liberdade de expressão e criar um ambiente seguro.

A IA é capaz de identificar e remover conteúdos que violam as diretrizes antes mesmo de serem denunciados, através de reconhecimento do conteúdo em fotos e analisar texto em publicações. Esses modelos podem identificar conteúdos explícitos ou impróprios, determinando se devem ser removidos ou ter sua distribuição reduzida. Em alguns casos, o conteúdo é encaminhado para uma análise mais detalhada por equipes humanas, que tomam as decisões finais.

Em conclusão, o papel de moderação de conteúdo das redes sociais é crucial, especialmente no que se refere ao conteúdo publicado por médicos. Muitas vezes, esses conteúdos podem entrar em conflito com as diretrizes e políticas da comunidade quando extrapolam o caráter educativo e se chocam com as proibições relativas a conteúdo de nudez, além de práticas enganosas e não validadas cientificamente. Nesse contexto, é imperativo que as plataformas mantenham uma postura vigilante e rigorosa, assegurando que a informação compartilhada seja precisa e ética. A

32. FACEBOOK. *Ajuda do Instagram: Como o Instagram usa inteligência artificial para moderar conteúdos*. Disponível em: <https://pt-br.facebook.com/help/instagram/423837189385631>. Acesso em: 24 jun. 2024.

moderação eficaz não só protege a integridade das informações de saúde, mas também resguarda a confiança do público, promovendo um ambiente digital seguro e informativo.

6. CONVERGÊNCIAS E DIVERGÊNCIAS ENTRE O PAPEL DE MONITORAMENTO DOS CONSELHOS REGIONAIS DE MEDICINA E A MODERAÇÃO DE CONTEÚDO EXERCIDA PELA META

Os tópicos anteriores apresentaram individualmente os aspectos do monitoramento de conteúdo realizado pelos Conselhos Regionais de Medicina (CRMs) e a moderação de conteúdo exercida pela Meta, no Instagram. Neste tópico, serão analisadas as convergências e divergências entre os papéis de cada um desses personagens.

A começar pelas convergências, tanto a Meta quanto os Conselhos Regionais de Medicina compartilham um objetivo em comum: a proteção do público. Essa convergência se manifesta nas políticas e ações que ambas implementam para garantir um ambiente seguro e informativo em relação aos conteúdos de saúde.

Os CRMs, através das Codames, além de zelar pelos princípios éticos da profissão, exercem o poder de monitorar e educar seus inscritos para promoverem conteúdos de saúde verdadeiros e informativos.

Por sua vez, a Meta adota políticas de moderação de conteúdo com o intuito de proteger seus usuários. Essas políticas visam a prevenção da desinformação, para criar um ambiente seguro, livre de conteúdos nocivos ou inadequados, como imagens explícitas, discurso de ódio e fraudes.

Portanto, a moderação de conteúdo das redes sociais e a fiscalização dos CRMs convergem na missão de garantir que as informações de saúde acessíveis ao público sejam precisas, seguras e benéficas. Essa sinergia é necessária para manter a integridade das informações de saúde na era digital, onde a disseminação rápida de conteúdos pode ter impactos significativos na saúde pública.

A segunda convergência é a avaliação do conteúdo publicado. É um aspecto essencial tanto para as redes sociais quanto para os CRMs, embora suas abordagens e fundamentos normativos sejam substancialmente distintos.

A Meta implementa um conjunto abrangente de políticas e ferramentas para moderar o conteúdo postado por seus usuários, como as Diretrizes da Comunidade e Política de Publicidade vistas no tópico anterior. Por sua vez, os CRMs monitoram o conteúdo relacionado à prática médica, incluindo o que é compartilhado nas redes sociais, com fundamento em resolução do próprio conselho profissional.

Outra divergência é a forma de atuação, enquanto a a Meta aplica suas políticas de forma ampla a todos os usuários, enquanto os conselhos regionais focam especificamente nos médicos e na prática médica.

Para a Meta a fiscalização se baseia em um conjunto de regras gerais que visam manter a plataforma segura para todos. As plataformas dependem tanto de revisões reativas (respondendo a denúncias de usuários) quanto de monitoramento proativo (algoritmos que detectam automaticamente violações). A escala global exige que as redes sociais implementem sistemas que possam lidar com um volume massivo de conteúdo.

A fiscalização dos CRMs, por outro lado, é específica e focada na prática médica dentro do contexto brasileiro. Fiscaliza exclusivamente os médicos registrados no Brasil, avaliando suas ações e comunicações com base em normas profissionais e éticas específicas. A fiscalização é detalhada e contextual, considerando as particularidades de cada caso.

Outra divergência é a consequência da atuação. A Meta pode remover conteúdo ou banir usuários, enquanto o CRM pode aplicar sanções profissionais que afetam diretamente a carreira dos médicos.

Por fim, a transparência e a responsabilidade na moderação de conteúdo e fiscalização são áreas onde as redes sociais e o CRM apresentam abordagens significativamente distintas.

Nas redes sociais, a transparência e a responsabilidade na moderação de conteúdo frequentemente enfrentam desafios como falta de transparência uma vez que as políticas de remoção de conteúdo, suspensão de contas e outras ações punitivas nem sempre são claramente comunicadas aos usuários. Esta falta de clareza pode gerar frustração e a percepção de que as decisões são arbitrárias ou inconsistentes.

Além disso, as plataformas de redes sociais possuem uma responsabilidade limitada perante os usuários. Embora existam mecanismos para apelação de decisões de

moderação, o processo pode ser complexo e pouco acessível. Além disso, a responsabilidade das plataformas é frequentemente mitigada por seus termos de serviço, que lhes conferem um amplo leque de ações discricionárias. As redes sociais dependem principalmente de revisões internas para resolver disputas sobre moderação de conteúdo. Isso levanta questões sobre a imparcialidade e a consistência das decisões, já que as revisões são conduzidas dentro da própria estrutura da empresa.

Os CRMs, em contraste, adotam uma abordagem procedimental em sua fiscalização. Apesar da tramitação sigilosa, o CRM segue processos bem definidos em resolução para investigar e julgar infrações éticas e profissionais. As denúncias contra médicos são cuidadosamente investigadas, e os médicos têm o direito de defesa e de apelação. As decisões são documentadas e podem ser revisadas por instâncias superiores.

Ambas as entidades, embora atuem de formas diferentes, compartilham a responsabilidade de combater a desinformação. Enquanto as redes sociais se concentram na identificação e remoção rápida de conteúdos falsos para proteger seus usuários, os CRMs garantem que os profissionais de saúde sigam padrões éticos rigorosos e promovam apenas informações verídicas. Juntas, essas ações ajudam a criar um ambiente mais seguro e informativo para todos.

Essas diferenças na transparência e responsabilidade destacam os distintos enfoques das redes sociais e dos Conselhos Regionais de Medicina. Enquanto as redes sociais enfrentam desafios em garantir a transparência e a percepção de justiça em suas decisões de moderação, o CRM opera com um processo ético-profissional, proporcionando maior confiança e previsibilidade em suas ações de fiscalização. Esse contraste é fundamental para compreender como cada entidade lida com a moderação e monitoramento de conteúdo.

7 PROPOSTA DE GOVERNANÇA COLABORATIVA

Conforme debatido até aqui, os Conselhos Regionais de Medicina e plataformas como a Meta (Instagram) possuem atuações distintas no ecossistema de avaliação de conteúdo de saúde publicado nas redes sociais por médicos.

Embora suas atribuições sejam diferentes, uma atuação conjunta pode representar uma estrutura de governança colaborativa mais eficiente para a curadoria de

conteúdos de saúde. Essa perspectiva surge da ideia de Evelyn Douek³³, que defende a necessidade de uma forma de governança mais proativa e contínua, além da simples correção de erros individuais.

A necessidade de uma vigilância regulatória eficaz é evidente, exigindo que os órgãos reguladores sejam proativos na fiscalização e aplicação das diretrizes estabelecidas pelas resoluções. Isso implica não apenas na detecção de violações, mas também na promoção de uma cultura de conformidade ética entre os profissionais de saúde.

A responsabilidade pela promoção de uma publicidade ética na medicina é compartilhada entre os profissionais de saúde, que devem garantir que suas práticas de publicidade estejam alinhadas com os princípios éticos, e a sociedade, que tem o direito de exigir transparência e honestidade nas informações de saúde.

George Salomão e Ronaldo Lemos³⁴ destacam que “*o Brasil tem uma importante trajetória de formulação de políticas que observam o caráter multisetorial, ouvindo e garantindo a participação dos mais diferentes atores.*” Para criar um ambiente saudável na internet, é essencial a colaboração entre médicos, plataformas de redes sociais e reguladores.

Um exemplo prático dessa estrutura colaborativa são os convênios firmados entre conselhos profissionais e autoridades para tratar de assuntos de saúde, como o Convênio entre o Conselho Regional de Medicina do Paraná e o Ministério Público do Estado do Paraná. Esse acordo visa a adequação de serviços médicos na região, com o compromisso de prestar orientação e apoio mútuo sempre que receberem reclamações contra médicos no exercício da profissão³⁵.

Tal iniciativa revela a possibilidade de criação de uma estrutura multisetorial para a promoção de uma governança colaborativa, destinada a avaliar, monitorar, moderar e promover conteúdo ético de saúde nas redes sociais.

Além disso, uma governança colaborativa também pode contar com a atuação da sociedade civil, representada pelos usuários das próprias plataformas. Informados

33. DOUEK, Evelyn. *Content Moderation as Systems Thinking*. Harvard Law Review. Cambridge: Harvard University Press. v. 136, n. 02, p. 526-607, Dec. 2022.

34. LEITE, George Salomão; LEMOS, Ronaldo. *Marco Civil da Internet*. São Paulo: Atlas, 2014.

35. SCHAEFER, Fernanda. *Responsabilidade Civil do Médico & Erro de Diagnóstico*. 1 ed (2002), 12 reimp. Curitiba: Juruá, 2022. p. 55

sobre os procedimentos e canais de denúncia, esses usuários podem sinalizar para as autoridades a existência de conteúdo de saúde impróprio ou enganoso.

Na prática, os usuários já realizam um modelo descentralizado de moderação. Além de denunciarem conteúdos, criam perfis cujo objetivo é divulgar conteúdo informativo com base científica e desconstituir informações errôneas publicadas por profissionais da saúde. Exemplos disso são os perfis de Instagram “nuncavilcientista”, gerenciado por Laura Marise³⁶ e Ana Bonassa³⁷.

João Quinelato, citado por Juliana Dantas (2019)³⁸, ressalta que os provedores de aplicação não têm o dever jurídico de controle editorial sobre o conteúdo postado, conforme entendimento do STJ, mas também não podem permanecer inertes diante de violações de direitos fundamentais. Eles devem adotar medidas proativas para prevenir e reprimir condutas ilícitas, observando um regime de responsabilidade civil que vai além da reparação patrimonial, cumprindo uma função social e de proteção da dignidade humana.

Portanto, apesar das várias fontes citadas, toda essa discussão só foi possível em razão do Marco Civil da Internet, que além dos seus objetivos de proteção do usuário e responsabilização de provedores, promove uma abordagem multissetorial que pode ser aplicada para garantir que o conteúdo publicado por médicos seja moderado de forma justa, segura e respeitosa, protegendo os direitos dos usuários e a dignidade dos pacientes.

Por sua vez, o CFM deve desempenhar um papel educativo contínuo, fornecendo orientações claras sobre a publicação de conteúdo nas redes sociais. Isso inclui capacitar os médicos sobre a importância de adotar comportamentos éticos e garantir que qualquer publicação respeite as regras do conselho profissional, do MCI e das políticas das plataformas.

36. <http://lattes.cnpq.br/2603023551856235>

37. <http://lattes.cnpq.br/4947742884022371>

38. DANTAS, Juliana de Oliveira Jota; MOTA NETO, Leonardo Lima. *Liberdade de Expressão versus Responsabilidade dos Provedores no Marco Civil da Internet*. Revista da AGU, Brasília, v. 21, n.º 04, p. 143-162, out./dez. 2022.

8 CONCLUSÃO

A evolução das diretrizes de publicidade médica, impulsionada pelo avanço tecnológico e a popularização das redes sociais, exige uma adaptação contínua das normas éticas e regulamentares. A Resolução CFM 2.336/2023 representa um passo significativo para garantir a transparência e a veracidade das informações de saúde divulgadas pelos profissionais médicos. No entanto, a eficácia dessas diretrizes depende de uma possível estrutura de colaboração entre os Conselhos Regionais de Medicina (CRMs), plataformas digitais como a Meta (Instagram), sociedade civil e outras autoridades de saúde.

Como visto, os Conselhos de Classe, como os CRMs, e as redes sociais, como a Meta, desempenham papéis distintos e atuam em esferas diferentes, um no monitoramento e outro na moderação de conteúdo de saúde. Enquanto os CRMs operam em uma esfera administrativa, focando na prática médica e aplicando sanções profissionais conforme as diretrizes éticas, as redes sociais seguem as políticas estabelecidas por empresas privadas, utilizando algoritmos e inteligência artificial para garantir a conformidade com suas normas.

Apesar dessas diferenças, as convergências entre suas missões de proteger o público e assegurar a veracidade das informações possibilitam a formação de uma estrutura colaborativa. Essa colaboração é essencial para enfrentar desafios comuns, promovendo um ambiente digital seguro, ético e informativo.

A atuação conjunta desses atores pode formar uma estrutura de governança colaborativa mais eficiente, que não apenas monitore, mas também eduque e oriente os profissionais de saúde sobre a comunicação ética nas redes sociais. A utilização de tecnologias de inteligência artificial para a moderação de conteúdo deve ser complementada por uma supervisão humana, garantindo que as nuances da prática médica sejam respeitadas.

A colaboração entre médicos, reguladores e plataformas é fundamental para criar um ambiente digital seguro, informativo e ético, que proteja tanto os profissionais de saúde quanto os pacientes.

Por fim, a promoção de uma cultura de conformidade ética na publicidade médica não é responsabilidade exclusiva dos CRMs ou das plataformas digitais. É um esforço conjunto que envolve também a sociedade civil e os próprios usuários das

redes sociais. Somente através de uma governança colaborativa e transparente será possível garantir que o conteúdo de saúde divulgado nas redes sociais contribua para o bem-estar e a informação correta da população.

REFERÊNCIAS

- BRASIL. Lei n.º 3.268, de 30 de setembro de 1957. Dispõe sobre os Conselhos de Medicina. Diário Oficial da União: Rio de Janeiro, 30 de set. 1957 Disponível em: https://www.planalto.gov.br/ccivil_03/LEIS/L3268.htm#art36. Acesso em: 24 jun. 2024.
- BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União: Brasília, DF, 23 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 08 jun. 2024.
- BREGA, Gabriel Ribeiro. *A Regulação de conteúdo nas redes sociais: uma breve análise comparativa entre o NetzDG e a solução brasileira*. Revista Direito GV. São Paulo: Direito GV, v. 19, n. 44, p. 01-27, mar. 2023.
- DANTAS, Eduardo. *Breves Apontamentos sobre a Publicidade e Propaganda na Atividade Médica em Seus Aspectos Éticos e Deontológicos. A Nova Resolução CFM Nº 2.336/2023*. Centro de Investigação de Direito Privado (CIDP). Artigo da Revista Jurídica Luso-Brasileira, v. 01, p. 139-188, 2024. Disponível em: https://www.cidp.pt/revistas/rjlb/2024/1/2024_01_0139_0188.pdf. Acesso em: 24 jun. 2024.
- CNN BRASIL. *Justiça condena defensores de tratamento precoce contra covid a pagar R\$ 55 milhões*. Disponível em: <https://www.cnnbrasil.com.br/saude/justica-condena-defensores-de-tratamento-precoce-contra-covid-a-pagar-r-55-milhoes/>. Acesso em: 24 jun. 2024.
- COMITÊ GESTOR DA INTERNET NO BRASIL. *Princípios para a Governança e Uso da Internet no Brasil*. Disponível em: <https://principios.cgi.br/>. Acesso em: 8 jun. 2024.
- CONSELHO FEDERAL DE MEDICINA (CFM). Resolução nº 2.217/2018. Código de Ética Médica. Diário Oficial da União: Brasília, DF, 2019. Disponível em: <https://portal.cfm.org.br/imagens/PDF/cem2019.pdf>. Acesso em: 24 jun. 2024.
- CONSELHO FEDERAL DE MEDICINA (CFM). Resolução CFM nº 2.306/2022. Aprova o Código de Processo Ético-Profissional (CPEP) no âmbito do Conselho Federal de Medicina (CFM) e Conselhos Regionais de Medicina (CRMs). Diário Oficial da União: seção I, Brasília, DF, 25 mar. 2022. Disponível em: https://portal.cfm.org.br/wp-content/uploads/2022/03/2306_2022.pdf. Acesso em 29. jun. 2024.
- CONSELHO FEDERAL DE MEDICINA (CFM). Resolução CFM nº 2.336/2023. Dispõe sobre publicidade e propaganda médicas. Diário Oficial da União: seção I, Brasília, DF, 13 set. 2023.

Disponível em: <https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2023/2336>. Acesso em 08. jun. 2024.

CONSELHO REGIONAL DE MEDICINA DO MARANHÃO (CRM-MA). Manual de Publicidade. Disponível em: <https://crmma.org.br/wp-content/uploads/2024/03/Manual-de-publicidade-completo-1.pdf>. Acesso em: 30 jun. 2024.

CONSELHO REGIONAL DE MEDICINA DO PARANÁ (CRM-PR). Antes e depois: por que não pode. Disponível em: <https://www.crmpr.org.br/Antes-e-depois-por-que-nao-pode-13-51491.shtml>. Acesso em: 24 jun. 2024.

DANTAS, Juliana de Oliveira Jota; MOTA NETO, Leonardo Lima. *Liberdade de Expressão versus Responsabilidade dos Provedores no Marco Civil da Internet*. Revista da AGU, Brasília, v. 21, n.º 04, p. 143-162, out./dez. 2022.

DOUEK, Evelyn. *Content Moderation as Systems Thinking*. Harvard Law Review. Cambridge: Harvard University Press. v. 136, n. 02, p. 526-607, Dec. 2022.

ESTADO DE MINAS. *SBCP suspende e exclui médicos por conduta nas redes: especialista explica*. Disponível em: https://www.em.com.br/app/noticia/bem-viver/2022/02/25/interna_bem_viver,1348304/sbcpsuspende-e-exclui-medicos-por-conduta-nas-redes-especialista-explica.shtml. Acesso em: 24 jun. 2024.

EXAME. *Médicos em vídeo banido nos EUA já negaram gravidade do coronavírus*. Disponível em: <https://exame.com/mundo/medicos-em-video-banido-nos-eua-ja-negaram-gravidade-do-coronavirus/>. Acesso em: 24 jun. 2024.

FACEBOOK. *Como o Instagram usa inteligência artificial para moderar conteúdos*. Disponível em: <https://pt-br.facebook.com/help/instagram/423837189385631>. Acesso em: 24 jun. 2024.

FACEBOOK BUSINESS. *Ajuda: Políticas de Publicidade*. Disponível em: <https://pt-br.facebook.com/business/help/248923537779939?id=434838534925385>. Acesso em: 24 jun. 2024.

INSPER. *Como funciona a Suprema Corte da moderação da Meta*. Disponível em: <https://www.insper.edu.br/noticias/como-funciona-a-suprema-corte-da-moderacao-da-meta/>. Acesso em: 24 jun. 2024.

INSTAGRAM. *Ajuda: Community Guidelines*. Disponível em: https://help.instagram.com/477434105621119?ref=igtos&helpref=faq_content. Acesso em: 24 jun. 2024.

LEITE, George Salomão; LEMOS, Ronaldo. *Marco Civil da Internet*. São Paulo: Atlas, 2014.

MULLIGAN, Deirdre, K.; BAMBERGER, Kenneth A. *Allocating Responsibility in Content Moderation: A Functional Framework*. Berkeley Technology Law Journal. Berkeley: University of California School of Law. v. 36, n. 03, p. 1091-1171, 2021.

SCHAEFER, Fernanda. *Responsabilidade Civil do Médico & Erro de Diagnóstico*. 1 ed (2002), 12 reimp. Curitiba: Juruá, 2022. p.

SHENG, Chuyi. *Automated Content Moderation*. Georgetown Law Technology Review. Washington:

Georgetown Law School. v. 06, n. 01, p. 351-363, Jun. 2022.

SIMPLÍCIO, A. H. *Social media and Dentistry: ethical and legal aspects*. Dental Press Journal of Orthodontics, v. 24, n. 6, p. 80-89, dez. 2019. DOI: 10.1590/2177-6709.24.6.080-089.sar. Disponível em: https://www.scielo.br/scielo.php?script=sci_arttext&pid=S217694512019000600080&lng=en&nrm=iso&tlng=en. Acesso em: 01 jun. 2024.

VALOR. *Justiça autoriza propaganda com antes e depois de pacientes*. Disponível em: <https://valor.globo.com/patrocinado/dino/noticia/2022/12/07/justica-autoriza-propaganda-com-antes-e-depois-de-pacientes-1.ghtml>. Acesso em: 29 jun. 2024.

VI

REGULAÇÃO DE PLATAFORMAS DIGITAIS: LIBERDADE DE EXPRESSÃO OU EXERCÍCIO DE PODER?

REGULAÇÃO DE PLATAFORMAS DIGITAIS: LIBERDADE DE EXPRESSÃO OU EXERCÍCIO DE PODER?

Laurence Duarte Araújo Pereira

Mestre e Doutorando em Direito pela UFMG. Sócio da Vilar Pereira Paiva e Real
Sociedade de Advogados.

Maelle Antunes Pereira Lima

Bacharel em Direito pela Faculdade de Direito Milton Campos. Especialista em
Direito do Trabalho pelo CAD. Advogada trabalhista na Sociedade de Advogados
Caldeira Brant.

Maria Cláudia Viana Hissa Dias do Vale Gangana

Mestre pela Faculdade de Direito Milton Campos. Doutoranda em Direito pela
UFMG. Advogada na Gangana Sociedade de Advogados. Professora do Centro
Universitário Estácio de Belo Horizonte.

DOI: <https://doi.org/10.59224/dti7.ch13>

Resumo: No cenário em que as plataformas digitais, entendidas neste trabalho como provedores de aplicações da internet, especialmente sob a ótica das redes sociais, extrapolaram a interação social e alcançaram os ambientes negociais, as questões afetas à moderação de conteúdos postados por seus usuários ganham novos contornos. No ordenamento jurídico brasileiro, a matéria foi regulamentada pelo Marco Civil da Internet e sustenta defesa na liberdade de expressão, cujo pano de fundo é constitucional. No entanto, a discussão em torno da constitucionalidade do artigo 19 da referida norma alcança o Supremo Tribunal Federal, sinalizando a possibilidade de ampliação da responsabilidade dos provedores de aplicação quanto aos conteúdos veiculados pelos usuários. Todavia, o debate merece reflexão, eis que, como será demonstrado, o exercício do poder, pelas plataformas digitais, pode ultrapassar o discurso de garantia das liberdades

Abstract: In a scenario in which digital platforms, understood in this paper as internet application providers, especially from the point of view of social networks, have gone beyond social interaction and reached business environments, issues related to the moderation of content posted by their users have taken on new contours. In the Brazilian legal system, the matter has been regulated by the Marco Civil da Internet (Civil Rights Framework for the Internet) and is defended on the basis of freedom of expression, whose background is constitutional. However, the discussion surrounding the constitutionality of article 19 of the Marco Civil has reached the Supreme Court, signaling the possibility of extending the responsibility of application providers for the content posted by users. The debate deserves reflection, though, because, as will be shown, the exercise of power by digital platforms

individuais.

Palavras-chave: Moderação de conteúdo; provedores de aplicação; Marco Civil da Internet.

can go beyond the discourse of guaranteeing individual freedoms.

Keywords: Content moderation, application providers, Internet Civil Rights Framework.

SUMÁRIO: 1. Introdução. 2. Marco civil da internet e regulação das plataformas digitais. 3. A constitucionalidade do artigo 19 do Marco Civil da Internet à luz dos temas 533 e 987 do Supremo Tribunal Federal. 4. A discussão da constitucionalidade do artigo 19 do Marco Civil da Internet sob a ótica da liberdade de expressão e os reais riscos na tomada do exercício de poder pelas plataformas digitais. 5. Conclusão. Referências.

1. INTRODUÇÃO

Recentemente, o controverso bilionário Elon Musk, CEO da Tesla Motors, fundador de empresas de tecnologia como a SpaceX, Neuralink, Starlink, comprador do antigo Twitter, cujo nome foi modificado para “X”, entrou em rota de colisão com o Supremo Tribunal Federal Brasileiro ao acusar a corte de promover a *censura* no uso da internet no Brasil.

A polêmica teve origem em uma publicação, realizada por Musk, na sua própria rede social, o X, em 6 de abril do ano corrente, como resposta à postagem publicada pelo Ministro Alexandre de Moraes, na qual ele parabenizava ao ex-Ministro daquela corte, Ricardo Lewandowski, em que Musk perguntava: *porque vocês estão demandando tanta censura no Brasil?*¹. Em resposta, a pedido da Procuradoria Geral da República, Moraes tornou Musk investigado no Inquérito n. 4957², que trata das

1. Disponível na rede X: <https://x.com/elonmusk/status/1776475718383534148>. Acesso em: 16 jun. 2024.

2. “Agora, a Procuradoria-Geral da República requereu o que segue: “Ao tempo em que dá ciência da decisão do dia 7 de abril último nestes autos, e tendo em vista o teor da deliberação e de notícias divulgadas na mídia desde ontem, o Ministério Público Federal entende pertinente que os representantes legais da rede “X” no Brasil sejam ouvidos para esclarecer se o Sr. Elon Musk detém, nos termos dos estatutos da empresa, atribuição para, sponte sua, determinar a publicação de

chamadas *fake news* e dos atos atentatórios ao regime democrático no Brasil.

Esse embate se dá no contexto em que se discute, no Brasil, a regulação das plataformas digitais, sobretudo pelo Projeto de Lei (PL) n. 2.630, de 2020, de autoria do Senador Alessandro Vieira, que tem por objetivo instituir a *Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet*, mas acabou sendo amplamente conhecido pelo apelido de *PL das Fake News*³, e do trâmite, no STF, dos Temas Repetitivos n. 533 e 987⁴.

Dessa forma, no Brasil, o debate da regulação das plataformas digitais passa, dentre outros fatores, pela análise de constitucionalidade do artigo 19 da Lei n. 12.965/2014 – mais conhecida como Marco Civil da Internet, que está em discussão nos referidos Temas Repetitivos, pelas ameaças à liberdade de expressão que esta

postagens na rede referida e se o fez, efetivamente, com relação a perfis vedados por determinação judicial brasileira em vigor. Ainda, que sejam ouvidos para que possam dizer se a empresa realizou algum levantamento do bloqueio de perfil até agora suspenso por determinação judicial. Se isso ocorreu, que informem quem competente para tanto no âmbito da empresa determinou o ato. Da mesma forma, se houve levantamento do bloqueio determinado por ordem judicial em vigor, que informem quais os perfis proscritos que voltaram a se tornar operantes.” Logo, para que a PGR melhor possa avaliar a situação objeto do Inq 4.957/DF, impõe-se o deferimento das medidas pleiteadas, haja vista que estão em conformidade com a investigação determinada para os fins da instauração de Inquérito, que objetiva apurar as condutas de Elon Musk, dono e CEO da provedora da rede social “X”. Assim, DEFIRO o requerido pela PGR: a) A oitiva dos representantes legais da rede “X” no Brasil “para esclarecer se o Sr. Elon Musk detém, nos termos dos estatutos da empresa, atribuição para, sponte sua, determinar a publicação de postagens na rede referida e se o fez, efetivamente, com relação a perfis vedados por determinação judicial brasileira em vigor”; b) “Que sejam ouvidos para que possam dizer se a empresa realizou algum levantamento do bloqueio de perfil até agora suspenso por determinação judicial”; c) “Se isso ocorreu, que informem quem competente para tanto no âmbito da empresa determinou o ato. Da mesma forma, se houve levantamento do bloqueio determinado por ordem judicial em vigor, que informem quais os perfis proscritos que voltaram a se tornar operantes”. STF. Inquérito 4.957. Rel. Min. Alexandre de Moraes. Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=6893258>. Acesso em: 17 jun. 2024.

3. BRASIL. Câmara dos Deputados. Projeto de Lei nº 2.630/2020. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2256735>. Acesso em: 17 jun. 2024.
4. STF. Tema 533. Disponível em: <https://portal.stf.jus.br/jurisprudenciaRepercussao/tema.asp?num=533>. Acesso em: 16 jun. 2024.

regulação pode representar e, ainda, pelos projetos legislativos já tramitados sobre o tema, tais como o PL n. 2.630/2020 e a extinta Medida Provisória n. 1.068/2021, além dos inúmeros debates públicos.

A discussão em torno das plataformas digitais alcançou proporções inimagináveis, eis que o uso crescente dos espaços virtuais, notadamente as redes sociais, não só como ferramenta comunicacional, mas também, como instrumento de trabalho e de influência social, viabilizou a interação entre as pessoas ao redor do globo, diluindo fronteiras e ampliando vertiginosamente as possibilidades de experiências culturais, filosóficas e sociais.

Emergiu, então, o que Manuel Castells chamou de comunicação de massa auto comandada, entendida como a comunicação de massa pelo seu potencial de difusão por toda a internet e, por consequência, propagação em todo o planeta. Auto comandada, porque *“geralmente é iniciada por indivíduos ou grupos, por eles próprios, sem a mediação do sistema de mídia”*⁵.

Se, por um lado, a comunicação em rede teve impactos positivos ao viabilizar interlocuções transfronteiriças, por outro, faz emergir danos em larga escala, resultantes da desinformação, dos chamados discursos de ódio e da interferência na tomada de decisão, pelas pessoas, incluindo-se, mas não se limitando aos processos eleitorais, o que terminou por intensificar os debates em torno da moderação de conteúdos veiculados por terceiros em provedores de aplicação, entre eles, as redes sociais.

A liberdade de expressão passa, então, a ser o pano de fundo constitucional para aqueles cuja regulamentação das plataformas digitais se revela como forma de ameaça ao estado democrático de direito e tem tomado papel preponderante no debate, ante a necessidade de preservação e garantia aos direitos individuais, coletivos, sociais e políticos, os quais também foram consagrados como fundamentos do Marco Civil da Internet, em sua base principiológica. No entanto, outros aspectos relevantes do debate têm sido deixados de lado, conforme se verá adiante. As manifestações públicas de relevantes agentes econômicos, como Elon Musk, defendendo a liberdade de expressão em meio a complexos debates regulatórios, demonstram o papel

5. CASTELLS, Manuel; CARDOSO, Gustavo (Orgs.). *A Sociedade em Rede: do conhecimento à ação política*; Conferência. Belém (Por): Imprensa Nacional, 2005. Pág. 22.

preponderante do tema.

O objetivo deste estudo será, neste sentido, demonstrar que a liberdade de expressão, por mais que seja extremamente relevante, é apenas um dos aspectos a ser observado no debate relativo à regulação das plataformas digitais. Para tanto, no tópico a seguir, far-se-á uma introdução sobre o Marco Civil da Internet, bem como sobre as suas disposições acerca da regulação das plataformas digitais no Brasil. Adiante, será realizada uma breve descrição sobre o julgamento da constitucionalidade do art. 19 do Marco Civil da Internet nos Temas Repetitivos nº 533 e 987, perante o STF. Em seguida, discutir-se-á o debate sobre a liberdade de expressão neste cenário regulatório, explorando, além da experiência brasileira, a experiência estadunidense, fundada, sobretudo, no art. 230 da *Communication Decency Act* (CDA). Por fim, a título de considerações finais, concluir-se-á que a liberdade de expressão não é o único tema em debate quando se fala em regulação das plataformas digitais.

Além disso, constata-se que, avaliando os demais aspectos jurídicos envolvidos no tema da regulação das plataformas digitais, é possível sustentar a constitucionalidade do art. 19, ou, quando menos, a sua interpretação conforme a Constituição, o que é fundamental para a manutenção de um ambiente de internet seguro e democrático no Brasil.

Esta conclusão traz, consigo, ainda, desafios para que medidas regulatórias concretas sejam tomadas no sentido de exigir que as empresas detentoras de plataformas digitais se organizem no sentido de garantir o cumprimento dos direitos de seus usuários, não se limitando à liberdade de expressão, mas também a outros direitos individuais e coletivos em jogo.

2. MARCO CIVIL DA INTERNET E REGULAÇÃO DAS PLATAFORMAS DIGITAIS

A Lei n. 12.965, de 2014, conhecida como Marco Civil da Internet, foi promulgada no Brasil sob atentos olhares da comunidade jurídica nacional e internacional, tendo por objetivo estabelecer princípios, garantias, direitos e deveres para o uso da internet no Brasil. Após participação ativa da sociedade civil, agentes de mercado, juristas e outros especialistas, o Marco Civil foi tido, ao tempo de sua publicação, por alguns, como uma lei que poderia servir de parâmetro para regulação da internet não só no

Brasil, mas também, em outros países⁶.

Como bem salientam Chiara Spadaccini de Teffé e Carlos Affonso Souza⁷, o texto normativo se inspirou não só na Constituição da República de 1988, atento aos princípios constitucionais expressamente elencados como basilares no uso da internet no Brasil, mas também, em um conjunto de recomendações do Comitê Gestor da Internet no Brasil⁸, que se preocupou em estabelecer diretrizes para a resolução de questões potencialmente conflituosas, garantindo direitos e deveres no mundo digital, pela inserção de normas especiais e gerais sobre o tema.

Dentre um dos princípios consagrados no Marco Civil da Internet, destaca-se a inimizabilidade de rede, pela qual os intermediários da internet à época, notadamente provedores de conexão e aplicações, não deveriam ser responsabilizados por ilícitos causados por seus usuários.

No Marco Civil, este princípio foi positivado, sobretudo, no artigo 19:

Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário.

§ 1º A ordem judicial de que trata o caput deverá conter, sob pena de nulidade, identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material.

§ 2º A aplicação do disposto neste artigo para infrações a direitos de autor

6. SALDÍAS, Osvaldo. Coded for Export! The Contextual Dimension of the Brazilian Marco Civil da Internet. Alexander von Humboldt Discussion Paper 2014-06. p. 01-24, nov. 2014.

7. TEFFÉ, C. S.; SOUZA, C. A. Responsabilidade civil de provedores na rede: análise da aplicação do Marco Civil da Internet pelo Superior Tribunal de Justiça. Revista IBERC, Belo Horizonte, v. 1, n. 1, p. 1-28, 2019. DOI: 10.37963/iberc. v1i1.6. Disponível em: <https://revistaiberc.emnuvens.com.br/iberc/article/view/6>. Acesso em: 26 jun. 2024.

8. COMITÊ GESTOR DA INTERNET NO BRASIL. Resolução CGI.br/RES/2009/003/P. Disponível em: <<https://www.cgi.br/resolucoes/documento/2009/003>>. Acesso em: 26 jun. 2024.

ou a direitos conexos depende de previsão legal específica, que deverá respeitar a liberdade de expressão e demais garantias previstas no art. 5º da Constituição Federal.

§ 3º As causas que versem sobre ressarcimento por danos decorrentes de conteúdos disponibilizados na internet relacionados à honra, à reputação ou a direitos de personalidade, bem como sobre a indisponibilização desses conteúdos por provedores de aplicações de internet, poderão ser apresentadas perante os juizados especiais.

§ 4º O juiz, inclusive no procedimento previsto no § 3º, poderá antecipar, total ou parcialmente, os efeitos da tutela pretendida no pedido inicial, existindo prova inequívoca do fato e considerado o interesse da coletividade na disponibilização do conteúdo na internet, desde que presentes os requisitos de verossimilhança da alegação do autor e de fundado receio de dano irreparável ou de difícil reparação.

Infere-se, a partir do dispositivo legal em comento, que a inimizabilidade de rede, com esteio na proteção à liberdade de expressão e na vedação da censura no âmbito das plataformas digitais, instaurou um ambiente de segurança aos provedores de aplicações de internet, responsáveis pela disponibilização de tais conteúdos na rede, na medida em que afasta a sua responsabilidade pelos danos decorrentes dos conteúdos postados por seus usuários, vinculando-a à existência de ordem judicial específica para a sua remoção, nos limites técnicos dos serviços prestados.

Desse modo, a partir da novel legislação, no ordenamento jurídico brasileiro, é possível afirmar que a responsabilidade das plataformas digitais, enquanto provedores de aplicações de internet, é subjetiva, eis que vinculada ao controle de legalidade, pelo poder judiciário, dos conteúdos gerados por terceiros, bem como dependente de ordem específica acerca da necessidade ou não da moderação, excetuado o disposto em lei em sentido contrário⁹.

9. Nesse sentido, destaca-se a redação atribuída ao artigo 21 do Marco Civil da Internet: Art. 21. O provedor de aplicações de internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante

Contudo, é necessário esclarecer que as discussões atinentes à moderação de conteúdo nas plataformas digitais têm suas origens antes mesmo da data da publicação do Marco Civil da Internet, eis que a utilização massiva das redes sociais, no Brasil, remonta ao ano de 2004, com a chegada do ORKUT, o que já permitiu entendimentos distintos daquele que restou positivado.

O Superior Tribunal de Justiça chegou a enfrentar o tema, cuja análise, ante a ausência de norma especial, submetia-se às diretrizes do Código de Defesa do Consumidor, considerando-se os conceitos de fornecedor e consumidor de produtos e serviços na Lei n. 8.078/1990. Nesse sentido, quando do julgamento do Recurso Especial n. 1.501.603/RN (2014/0290071-6)¹⁰, a Corte Superior entendeu que, considerando as atividades exercidas pelos provedores de aplicações de internet, a análise de tais conteúdos não estaria abrangida na sua atuação, de modo que não se poderia considerar tal serviço defeituoso, nos termos do artigo 14 da legislação consumerista, por ausência da moderação, aplicando-se, à época, a teoria da responsabilidade subjetiva¹¹.

Todavia, é preciso salientar que, nos processos ajuizados com base em fatos ocorridos anteriormente à vigência do Marco Civil da Internet, é possível constatar o reconhecimento da responsabilidade solidária das plataformas digitais, a partir do

ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo. Parágrafo único. A notificação prevista no caput deverá conter, sob pena de nulidade, elementos que permitam a identificação específica do material apontado como violador da intimidade do participante e a verificação da legitimidade para apresentação do pedido.

10. STJ, RE n. 1.501.603/RN. Rel(a). Min. Nancy Andrighi. DJe: 18 dez. 2017. Disponível em: https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1668833&num_registro=201402900716&data=20171218&formato=PDF. Acesso em: 26 jun. 2024.

11. Nesse sentido, o acórdão em referência no texto faz menção aos julgamentos ocorridos nos autos dos seguintes processos: REsp 1.308.830/RS (Terceira Turma, julgado em 08/05/2012, DJe 19/06/2012), REsp 1316921/RJ (Terceira Turma, julgado em 26/06/2012, DJe 29/06/2012), REsp 1568935/RJ (Terceira Turma, julgado em 05/04/2016, DJe 13/04/2016), AgRg no AREsp 614.778/RJ (Terceira Turma, julgado em 05/02/2015, DJe 12/02/2015), AgRg no AREsp 308.163/RS (Quarta Turma, julgado em 14/05/2013, DJe 21/05/2013) e AgRg no REsp 1.402.104/RJ (Quarta Turma, julgado em 27/05/2014, DJe 18/06/2014)

conhecimento da violação a direitos de terceiros, ainda que por meio de notificação extrajudicial, hipótese em que elas teriam se mantido inertes na remoção de tais conteúdos em discussão.

A título ilustrativo, destaca-se o julgamento ocorrido nos autos do Recurso Especial n. 1.512.647-MG (2013/0162883-2)¹², de relatoria do Ministro Luís Felipe Salomão, no qual se adotou o entendimento de que, para fatos pretéritos à legislação especial, a responsabilidade civil dos provedores de aplicações à internet pelos conteúdos postados por terceiros não depende de notificação judicial, sendo suficiente a prova da ciência da plataforma e de sua inércia na moderação. De acordo com o referido julgamento, embora a plataforma digital não tivesse a obrigação de analisar os conteúdos de seus usuários, a partir do conhecimento da ilegalidade, ainda que pela via extrajudicial, ela teria o dever de removê-los em prazo razoável.

A demarcação de contextos normativos e históricos, anteriores e/ou posteriores ao Marco Civil da Internet, terminou por aprofundar a discussão sobre o tema e intensificar as divergências, em escala proporcional à intensificação da utilização das plataformas digitais pelas pessoas ao redor do mundo, com debates acalorados entre regulamentação e liberdades.

A discussão se torna ainda mais sensível, eis que, reiteradamente, com base na sua capacidade de autorregulamentação, cujos interesses econômicos terminam se sobrepondo aos valores e princípios constitucionais, como bem salienta Ana Frazão¹³, as plataformas digitais vêm adotando critérios pouco claros, com base nos seus termos de uso, para garantir a moderação de conteúdo, na forma que melhor lhes convém, ainda que em sentido contrário ao disposto no Marco Civil da Internet¹⁴.

12. STJ. Recurso Especial n. 1.512.647-MG. Rel. Min. Luís Felipe Salomão. DJe 15 ago. 2015. Disponível em https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ATC&sequencial=45693836&num_registro=201301628832&data=20150805&tipo=91&formato=PDF. Acesso em: 26 jun. 2024.

13. FRAZÃO, Ana. Plataformas digitais e os desafios para a regulação jurídica. In: Parentoni, Leonardo (Coord.). Direito, tecnologia e inovação. Belo Horizonte: Editora D'Plácido, 2018. Disponível em: https://www.academia.edu/37773223/Plataformas_digitais_e_os_desafios_para_a_regulacao_C3%A7%C3%A3o_jur%C3%ADdica. Acesso em: 26 jun. 2024.

14. Sobre o assunto, destaca-se o julgamento ocorrido nos autos do AREsp nº 1595492 / SP, em que o Superior Tribunal de Justiça manteve a condenação do Facebook

Destarte, restam dúvidas concretas quanto aos ganhos efetivos na atribuição de tais responsabilidades às plataformas digitais. Gabriel Ribeiro Brega¹⁵, a partir de uma análise comparativa entre o NetzDG - legislação alemã controversa que adotou procedimentos específicos para a moderação de conteúdos nas plataformas digitais, inclusive com a fixação de multas substanciais para aquelas que descumprissem de forma reiterada os seus deveres de transparência e demais obrigações fixadas pela norma - e a experiência brasileira, constatou a ausência de relação direta entre moderação de conteúdo e a eficiência de um sistema rígido de controle. O referido autor destacou, ainda, os riscos efetivos à liberdade de expressão, quando o sistema atribui às plataformas digitais o exercício hermenêutico quanto à interpretação da lei, com a exclusão de tal competência do Poder Judiciário.

No entanto, no referido trabalho, não passou despercebida a necessidade de aperfeiçoamento das plataformas digitais no Brasil, como meio de melhorar as suas diretrizes e procedimentos, garantindo uma melhor experiência aos usuários, mais célere e transparente, em complemento à norma brasileira que restringe o autocontrole e atribui o exame de legalidade dos conteúdos e a ordem de remoção ao Estado:

A norma brasileira tem o mérito de privilegiar a liberdade de expressão do usuário, repelindo a lógica da exigência de censura prévia dos conteúdos pelo provedor - embora não impeça a adoção de controles internos pelas plataformas com base em suas próprias políticas. Não há, porém, exigências relativas a essas estruturas de controles internos. Parte da doutrina critica essa solução, pois, dada a morosidade da apreciação judicial, e, inversamente, a celeridade dos compartilhamentos em redes sociais, a publicação pode se propagar e o dano se intensificar (TEFFÉ e MORAES, 2017). No entanto, é justamente essa lógica que impede que a decisão a respeito

ao pagamento de multa no valor total de 254 mil reais, tendo em vista o não cumprimento de ordem judicial que determinou a reativação de um perfil na rede social Instagram, cuja exclusão se deu sem a devida motivação. Disponível em: <https://processo.stj.jus.br/processo/pesquisa/?aplicacao=processos.ea&tipoPesquisa=tipoPesquisaGene-rica&termo=AREsp%201595492>. Acesso em: 26 jun. 2024.

15. BREGA, Gabriel Ribeiro. A regulação de conteúdo nas redes sociais: uma breve análise comparativa entre o NetzDG e a solução brasileira. *Revista Direito GV*, São Paulo, v. 19, e2305, 2023. <https://doi.org/10.1590/2317-6172202305>. Acesso em: 26 jun. 2024.

do que é ou não ilegal seja delegada a agentes privados. Os provedores podem remover conteúdos porque estes violam suas políticas internas (que podem, em maior ou menor medida, refletir disposições legais), mas não porque foram incumbidos, pela lei, de aferir se determinadas condutas são ou não ilegais. Todavia, a norma alemã aposta nas estruturas e nos controles internos dos próprios provedores. Com isso, garante maior celeridade à análise e à eventual remoção de conteúdos, e evita o aprofundamento do dano com a permanência ou replicação da publicação. Entretanto, essa lógica acaba por atribuir aos agentes privados a decisão sobre a legalidade das publicações, encarregando-os, inclusive, de associar as condutas a tipos penais previstos no ordenamento jurídico alemão. A isso, soma-se o risco de over-blocking, anteriormente exposto, diante do receio de recebimento de multas.¹⁶

Diante de tal contexto conflituoso e de interpretações diversas sobre o tema, a capacidade das plataformas digitais de inflamar os episódios associados à desinformação, os discursos de ódio, as interferências em processos eleitorais¹⁷, acarretou consequências políticas e sociais expressivas, intensificando o debate acerca da moderação de conteúdos veiculados em provedores de aplicação e reforçando a ideia de que é necessário criar novos mecanismos regulatórios.

Na vanguarda desse movimento, a União Europeia aprovou o texto final do *Digital Services Act*¹⁸, que buscou promover o bom funcionamento dos serviços digitais, por meio de um espaço digital mais seguro e transparente.

Quanto à moderação de conteúdos veiculados *online*, atribuiu a responsabilidade desta atividade, essencialmente, aos provedores de serviços intermediários¹⁹,

16. BREGA, Gabriel Ribeiro. *Op. Cit.* p. 17.

17. Exemplos destes fatos foram mencionados no Jornal da USP de 10.03.2023, disponível em <https://jornal.usp.br/atualidades/e-possivel-combater-a-desinformacao-e-os-discursos-de-odionna-internet/>. Acesso em: 14 jun. 2024.

18. A lei foi aprovada em novembro de 2022 e o seu inteiro teor está disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ%3AL%3A2022%3A277%3ATOC&uri=uriserv%3AOJ.L_.2022.277.01.0001.01.ENG. Acesso em: 14 jun. 2024.

19. A lei, em seu art. 3º, conceituou “moderação de conteúdo” como sendo “as atividades, automatizadas ou não, empreendidas por prestadores de serviços intermediários, destinadas em especial a

escalonando obrigações de diligência de acordo com a categoria em que o destinatário se enquadra²⁰. Aplicável a partir de fevereiro de 2024, apesar de servir como modelo para possíveis regulações futuras em virtude de seu pioneirismo, seria prematuro tecer afirmações sobre o real impacto desta regulação nos mercados digitais.

Voltando à realidade brasileira, a regulação da matéria segue definida no art. 19 do Marco Civil da Internet, mas, na contramão da União Europeia, discute-se a constitucionalidade da norma perante pelo Supremo Tribunal Federal a partir de dois casos, como exposto na introdução, um anterior à legislação especial e o outro posterior à sua edição, exatamente na linha das divergências salientadas ao longo deste tópico.

Pretendeu-se, portanto, explorar neste tópico como, ao longo dos 10 (dez) anos de vigência do Marco Civil, a *inimputabilidade* de rede se tornou mais complexa, na medida em que os intermediários da internet, notadamente as plataformas digitais operadoras de redes sociais, tais como o Facebook, Instagram e outras, tornaram-se cada vez mais atuantes no modelo de negócio de direcionamento de conteúdo mediante o tratamento de dados, o que culminou na discussão de constitucionalidade do artigo 19 do Marco Civil da Internet.

3. A CONSTITUCIONALIDADE DO ARTIGO 19 DO MARCO CIVIL DA INTERNET À LUZ DOS TEMAS 533 E 987 DO SUPREMO TRIBUNAL FEDERAL

Diante do protagonismo alcançado pelas plataformas digitais no mercado, como demonstrado, antes mesmo da vigência do Marco Civil da Internet, discutia-se acerca da responsabilidade civil dos provedores de aplicações em virtude dos danos

detectar, identificar e combater os conteúdos ilegais ou informações incompatíveis com os seus termos e condições fornecidos pelos destinatários do serviço, incluindo as medidas tomadas que afetam a disponibilidade, visibilidade e acessibilidade desses conteúdos ilegais ou dessas informações, como a despromoção, a desmonetização, a desativação do acesso ou a supressão dos mesmos, ou que afetem a capacidade de os destinatários do serviço fornecerem essas informações, como a cessação ou suspensão da conta de um destinatário”.

20. A lei seccionou os provedores em quatro categorias, que são serviços intermediários, serviços de hospedagem, plataformas em linha e plataformas em linhas de grande dimensão.

decorrentes dos conteúdos gerados por seus usuários em face de terceiros, haja vista a inegável lucratividade da atividade. Essa é a discussão proposta no tema n. 533 perante o Supremo Tribunal Federal.

Dentre as correntes possíveis, defendeu-se que os provedores de aplicação, por se configurarem como meros intermediadores do conteúdo, não teriam qualquer tipo de responsabilidade, ante a ausência de nexo de causalidade entre a atividade e o prejuízo sofrido decorrente da postagem realizada por terceiros. Todavia, essa corrente terminou sendo repelida no ordenamento jurídico brasileiro, especialmente em razão de os processos terem origem, cotidianamente, em juizados especiais das relações de consumo, manejados por consumidores, cuja honra teria sido objeto de deboche em redes sociais, sem a intervenção das plataformas, mesmo quando acionadas extrajudicialmente.

Emergiu, então, a teoria da responsabilidade civil objetiva, calcada não só no disposto no Código de Defesa do Consumidor, que prevê o dever do fornecedor de produtos e serviços de reparar os danos causados em decorrência da sua atividade empresarial, independentemente da configuração de culpa, em quaisquer das suas modalidades, mas também, da já consolidada teoria do risco da atividade empresarial, preceituada no parágrafo único do artigo 927 do Código Civil, segundo a qual o exercício da empresa carrega consigo risco inerente à atividade.

Mas, com a vigência do Marco Civil da Internet, a discussão recebeu novos rumos diante da redação atribuída ao artigo 19 da referida Lei, que passou a delimitar a responsabilidade civil dos provedores de aplicação às hipóteses em que ficar configurada a inércia quanto à remoção do conteúdo em discussão, após o recebimento de notificação judicial e desde que observados os limites tecnológicos da plataforma respectiva. Em outras palavras, a partir da citada legislação, por expressa disposição normativa, a responsabilidade civil dos provedores de aplicação foi limitada e tornou-se subjetiva, devendo ser auferida em momento posterior ao controle de legalidade de conteúdo, pelo poder judiciário.

A partir desse novo contexto normativo, passou-se, então, a discutir eventual restrição aos direitos dos consumidores e, por conseguinte, a própria constitucionalidade do art. 19 do Marco Civil da Internet, atualmente pendente de análise pelo Supremo Tribunal Federal no Tema 987.

É importante ressaltar que os argumentos utilizados por quem sustenta o pedido declaratório de inconstitucionalidade do dispositivo suplanta a defesa do consumidor, mas termina por alcançar a Constituição da República de 1988, mais especificamente em seu capítulo sobre direitos fundamentais, porquanto a determinação contida no artigo 19 do Marco Civil da Internet, sob essa ótica, colidiria com os princípios da intimidade, da privacidade, além de fulminar direitos da personalidade, tais como o direito à honra e à imagem, também protegidos pela Carta Magna. A discussão se torna ainda mais ousada, visto que, por outro lado, aqueles que sustentam a validade da norma infraconstitucional, também se apoiam em princípios constitucionais consolidados, fortemente defendidos no cenário brasileiro, a exemplo da liberdade de expressão e vedação à censura.

Apesar de notáveis os argumentos sustentados por ambos os lados, se analisada a questão de modo mais aprofundado, constata-se que a discussão suplanta tais princípios alcança outras questões, afetas ao poder de influência de determinação social atribuído às plataformas na sociedade atual.

Isso porque, no atual momento social, os provedores de aplicações alçaram um patamar de importância outrora inimaginável, centrados no mercado da informação, aptos a influenciar pessoas, decidir quais são as informações que chegam até elas, impondo padrões e opiniões, capazes de alterar substancialmente mercados e sociedades.

A questão afeta à responsabilidade civil dos provedores foi um dos temas mais debatidos no processo participativo que antecedeu a aprovação do texto final do Marco Civil da Internet. Somente na segunda fase da consulta pública online foram recebidas 1.168 contribuições das quais mais de 200 tiveram como objeto o regime de responsabilidade civil atribuída aos provedores.²¹

O modelo de “*notice and counter notice*” estabelecido no texto inicial do Projeto de Lei foi alvo de críticas à época pelo fato de prescindir do filtro judicial, o que poderia ensejar remoções excessivas de conteúdo em violação à liberdade de

21. JOBIM, Nelson. LEMOS, Renato. PARECER. In. CONJUR. *Recurso Extraordinário questiona Marco Civil da Internet no STF*. 9 dez. 2019. Disponível em: <https://www.conjur.com.br/wp-content/uploads/2023/09/clique-aqui-ler-parecer-ronaldo-lemos.pdf>. Acesso em: 25 jun. 2024.

expressão.²² Nesta hipótese, o provedor atuaria como mero intermediário das partes envolvidas (notificante e notificado). Por outro lado, a proposta apresentada no texto final recebeu amplo apoio da sociedade civil, a exemplo do manifesto denominado “*Em defesa do Marco Civil*” assinado por várias entidades nacionais²³. Além disso, a ONU registrou em seu relatório sobre a liberdade de expressão que o Marco Civil se destaca pelo “*equilíbrio entre as liberdades na internet e coibição de ilícitos*”²⁴.

O legislador ordinário, de fato, buscou equilibrar os interesses em cena e, partindo do fundamento da liberdade de expressão e da inibição da censura, condicionou a responsabilização dos provedores de aplicação²⁵ por conteúdo danoso gerado por terceiro ao eventual descumprimento de decisão judicial.

Assim, o artigo 19 da Lei estabeleceu a responsabilidade civil subjetiva dos provedores e privilegiou a reserva de jurisdição quanto à moderação de conteúdo, contrariando a jurisprudência do STJ antecedente à sua promulgação. Diante disso, o Poder Judiciário “*foi considerado a instância legítima para definir a eventual ilicitude do conteúdo questionado e para construir limites mais legítimos para a expressão na rede.*”²⁶

Como já dito, a regra da reserva de jurisdição foi excetuada no art. 21 do Marco Civil, que atribuiu tratamento diferenciado para os casos de compartilhamento de “*imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado*” sem autorização de seus participantes, comumente conhecido como pornografia de vingança (*revenge porn*). Na hipótese, prevalece a lógica do

22. *Idem*.

23. “As entidades ressaltaram que a medida adotada no art. 19 delimita de forma justa e lúcida a responsabilidade dos intermediários na internet, evitando a censura prévia de conteúdos e privilegiando a liberdade de expressão e o direito à informação” INTERVOZES. *Em defesa do Marco Civil*. Disponível em: <https://intervozes.org.br/em-defesa-do-marco-civil/>. Acesso em: 28 jun. 2024.

24. JOBIM, Nelson. LEMOS, Ronaldo. *Op. Cit.*

25. A Lei 12.965/14 adotou uma classificação dicotômica, dividindo em provedores de conexão e provedores de aplicação, conforme se extrai do art. 11 *caput* e parágrafo 3º. Não obstante, existem classificações mais abrangentes, como as definidas por Marcel Leonardi.

26. SOUZA, Carlos Affonso Pereira de; LEMOS, Ronaldo. *Marco Civil da Internet: Construção e Aplicação*. Juiz de Fora: Editar, 2016, pág. 102.

*“notice and take down.”*²⁷

Em 2017, o senador Paulo Bauer (PSDB/SC) apresentou o Projeto de Lei nº 323 com o objetivo de alterar o art. 21 do Marco Civil, ampliando as hipóteses que exce- tuam a regra prevista no art. 19. No entanto, disponibilizada para consulta pública por meio do e-cidadania, o PLS teve apenas 155 votos a favor e 2.862 votos contra e, em 2018, a proposta foi retirada de pauta pelo autor.²⁸

De fato, a sistemática definida no art. 19 se mostra equilibrada e ajustada aos prin- cípios constitucionais e preocupações predominantes ao tempo da promulgação da Lei²⁹, quando se buscava *“preservar as bases para a promoção das liberdades e dos direitos na Internet no Brasil, distanciando-se assim de uma regulação repressiva da rede”*³⁰. Entretanto, a discussão acerca da responsabilidade civil dos provedores de aplicação tomou nova direção diante dos Temas em julgamento no STF.

No Tema 533, que precede a entrada em vigor da Lei 12.965/14, caberá à Suprema Corte definir se a empresa hospedeira de sítio na internet tem o dever de *“fiscalizar o conteúdo publicado e de retirá-lo do ar quando considerado ofensivo, sem interven- ção do Judiciário.”*³¹

O Tema 987, oriundo do *leading case* RE nº 1.037.396/SP, por outro lado, tem como núcleo controvertido a *necessidade de prévia e específica ordem judicial de*

27. Esta sistemática condiciona a atribuição de responsabilidade civil aos provedores à inércia na re- tirada ou moderação de conteúdo após mera notificação do usuário que se sinta lesado. Com isso, delega o monitoramento e decisão acerca da retirada de conteúdo aos provedores. Este modelo foi adotado, por exemplo, pela legislação alemã, NetzDG, e pelo DMCA (Digital Millenium Co- pyright Act) norte-americano.

28. BRASIL, Senado Federal. *Projeto de Lei n. 232, de 2017*. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/130820>. Acesso em: 28 jun. 2024.

29. Em 2015, a modalidade adotada no art. 19 do Marco Civil foi incorporada nos Princípios de Ma- nila, que buscaram promover práticas para limitar a responsabilidade dos prestadores de serviços intermediários e viabilizar a liberdade de expressão e inovação. Disponível em <https://manilaprin- ciples.org/pt-br>. Acesso em: 25 mai. 2024.

30. SOUZA, Carlos Affonso Pereira de; LEMOS, Ronaldo. *Marco Civil da Internet: Construção e Aplicação*. Juiz de Fora: Editar, 2016, pág. 16.

31. STF, Tema 533. Rel. Min. Luiz Fux. Disponível em: <https://portal.stf.jus.br/jurisprudenciareper- cussao/verAndamentoProcesso.asp?incidente=5217273&numeroProcesso=1057258&classePro- cesso=RE&numeroTema=533>. Acesso em: 29 jun. 2024.

*exclusão de conteúdo para a responsabilização civil de provedor de internet, websites e gestores de aplicativos de redes sociais por danos decorrentes de atos ilícitos praticados por terceiros*³².

Neste caso, a ação judicial, movida por usuária do Facebook Serviços Online do Brasil, teve como causa de pedir a criação de perfil falso em nome da autora no referido provedor. Por meio do perfil eram veiculadas postagens que, segundo a autora, abalaram a sua imagem e honra³³. Diante disso, a autora pleiteou a concessão de medida liminar para exclusão imediata do perfil falso, com cominação de multa em caso de descumprimento, além do fornecimento de informações da pessoa que criou a página, incluindo o IP (*Internet Protocol*) de origem, e indenização por danos morais.

O juízo da vara única do Juizado Especial de Capivari concedeu a tutela antecipada e determinou a retirada imediata do perfil falso. Na sentença, condenou o Facebook a apresentar o IP relativo ao perfil suprimido e confirmou a tutela antes concedida. Pautando-se nos artigos 18 e 19 do Marco Civil da Internet, foi julgado improcedente o pedido correlato à indenização por danos morais, com a ponderação de que o conteúdo não era flagrantemente ilícito, motivo pelo qual se entendeu que a plataforma agiu adequadamente ao aguardar a apreciação do Poder Judiciário³⁴.

Com este resultado, as partes interpuseram recurso inominado, distribuído para a 2ª Turma Recursal Cível do Colégio Recursal de Piracicaba/SP. Houve, com isso, a reforma parcial da sentença, para acrescer à condenação o pagamento de indenização por danos morais em desfavor do Facebook, justificando que estão caracterizados *in re ipsa*.

Observa-se do acórdão que os julgadores subverteram a lógica da reserva de jurisdição inscrita no art. 19 do Marco Civil, relativizando a sua aplicação sob a

32. STF, Tema 987. Rel. Min. Dias Tóffoli. Disponível em <https://portal.stf.jus.br/jurisprudenciaRepercussao/tema.asp?num=987> Acesso em: 28 mai. 2024.

33. Foi noticiado na petição inicial que “a conta intitulada como sendo da demandante consigna informações como a de que ela está esperando as pessoas para fazer fofquinhas, que isso melhora sua pressão arterial, que vai viajar com o circo, que é uma bêbada, que pegava dinheiro da aposentadoria da mãe e não lhe repassava, mas sim, o usou para reforma de seu imóvel, e mais inúmeros outros fatos”. STF, Tema 987. Rel. Min. Dias Tóffoli. Disponível em: <https://encurtador.com.br/eXTRP>. Acesso em: 21 mai. 2024.

34. *Idem*.

justificativa do esvaziamento do direito à “*efetiva prevenção e reparação de danos patrimoniais e morais*”, conforme trecho que segue transcrito³⁵:

Para fins indenizatórios, todavia, condicionar a retirada do perfil falso somente após ordem judicial específica, na dicção desse artigo, significaria isentar os provedores de aplicações, caso da ré, de toda e qualquer responsabilidade indenizatória, fazendo letra morta do sistema protetivo haurido à luz do Código de Defesa do Consumidor, circunstância que, inclusive, aviltaria preceito constitucional (art. 5º, inciso XXXII, da Constituição Federal). Ademais, tal disposição como que quer obrigar, compelir o consumidor vitimado, a ingressar em Juízo para atendimento da pretensão que, seguramente, poderia ser levada a cabo pelo próprio provedor cercando-se de garantias a fim de preservar, em última análise, a liberdade de expressão. Antes, o provedor fica em confortável, mas não menos desproporcional, posição de inércia frente à vítima do abuso desse mesmo direito de manifestação e pensamento, gerando paradoxal desequilíbrio em relação aos invioláveis direitos à intimidade, a vida privada, a honra e a imagem (art. 5º, inciso X, da Constituição Federal) desta última (vítima). Inegável que na relação entre as litigantes a autora, diante de sua notória condição de vítima, equipara-se à figura do consumidor (art. 17 do Código de Defesa do Consumidor). (...) Destarte, condicionar a responsabilização da ré à prévia tomada de medida judicial pela autora, na conformidade do art. 19 do Marco Civil da Internet, fulminaria seu direito básico de efetiva prevenção e reparação de danos patrimoniais e morais, individuais, coletivos e difusos (art. 6º, inciso VI, do Código de Defesa do Consumidor). Logo, a indenização pelos danos morais é medida que se impõe (...) (grifo nosso).

Para os julgadores a sistemática criada pelo art. 19 isenta “*os provedores de aplicação de toda e qualquer responsabilidade indenizatória*”. Essa percepção não parece adequada. Apesar de ter sido adotado um modelo de responsabilização menos severo do que aquele definido no Código do Consumidor, que pressupõe a responsabilidade civil objetiva, não significa que o provedor está imune dentro da relação jurídica.

O legislador, na verdade, privilegiou a inafastabilidade da apreciação do Poder

35. *Idem*.

Judiciário em caso de lesão ou ameaça de lesão, tal como preceituado no art. 5º, XXXV da Constituição. Assim, o dever de indenizar foi atribuído ao ofensor direto, cabendo ao provedor a responsabilidade subsidiária em caso de descumprimento de decisão judicial.

Parece relevante, aqui, a ideia de que “*um direito constitucionalmente previsto não necessariamente se projeta em um modelo de responsabilidade civil mais severo pela legislação infraconstitucional.*”³⁶ Nesse sentido, Rodrigo Leonardo destaca que, embora a Constituição estabeleça o direito e garantia fundamental à vida no caput do art. 5º, a indenização por dano à vida, em situações muitas vezes trágicas, se dá pela responsabilidade civil subjetiva, menos severa que outros modelos³⁷.

Outro aspecto a ser considerado é o fato de que um modelo de responsabilização mais severo pode inibir a disponibilização de “ferramentas abertas a edição e manipulação do público”, engessando a oferta de novos modelos de negócio pautados em novas tecnologias, o que trava a inovação e viola o princípio da livre iniciativa (art. 170 da CR/88)³⁸.

O Tribunal também justifica que a Lei quer “*compelir o consumidor vitimado, a ingressar em Juízo para atendimento da pretensão*”. Nesse sentido, parece partir da premissa de que o art. 19 condiciona a reparação ao crivo do Poder Judiciário, obrigando o usuário a sempre invocar a prestação jurisdicional para ter o seu direito atendido.

Não obstante, o Marco Civil não inviabiliza os provedores de aplicação de formularem regras próprias de moderação de conteúdo em seus termos de uso, ocasião em que a análise e possível remoção do material danoso ocorrerá sem a intervenção do Estado-juiz. Nesses casos, portanto, a avaliação do conteúdo compartilhado fica a cargo exclusivo do provedor.

Os relatórios de transparência (*transparency reports*) emitidos pelos próprios

36. LEONARDO, Rodrigo Xavier. *Controle de constitucionalidade do Marco Civil da Internet em audiência no STF*. In CONJUR. 3 abr. 2023. Disponível em: <https://www.conjur.com.br/2023-abr-03/direito-civil-atual-audiencia-publica-stf-controle-constitucionalidade-marco-civil-internet/>. Acesso em: 28 mai. 2024.

37. *Idem*.

38. JOBIM, Nelson. LEMOS, Ronaldo. *Op. Cit.*

provedores fornecem um panorama quantitativo das atividades de moderação realizadas, de onde é possível inferir que há atuação expressiva nesse campo. No período compreendido entre julho e dezembro de 2021³⁹, por exemplo, o *Twitter* (atual “X”) realizou de forma autônoma a suspensão de 1.3 milhões de contas e removeu 5.1 milhões de conteúdos, em cumprimento às suas políticas internas de uso.⁴⁰

No mesmo período, o relatório também noticia que a plataforma acionou diretamente determinados usuários para que removeassem 4 milhões de postagens veiculadas em violação às regras da plataforma.⁴¹ O documento secciona a intervenção direta da plataforma na moderação em três temas gerais: 1) segurança (violência terrorismo/extremismo violento exploração sexual de menores, comportamento abusivo, condutas de ódio, promoção de suicídio e automutilação, informações sensíveis incluindo violência gráfica e conteúdo adulto, bens ou serviços ilegais; 2) privacidade (informação privada e nudez não consensual) e 2) autenticidade (integridade cívica, falsificação de identidade, informação enganosa sobre COVID-19)⁴². Conclui-se, pois, que os provedores já adotam uma postura ativa em relação ao filtro dos conteúdos veiculados em suas plataformas.

Ao lado disso, tanto na hipótese prevista no art. 21, quanto nos casos de infrações a direitos de autor ou a direitos conexos⁴³ o provedor deverá agir de forma imediata, logo após a notificação extrajudicial. Esta estratégia legislativa é ponderada, pois modula o regime jurídico da reserva de jurisdição a situações específicas, em que a identificação da ilegalidade do conteúdo pode ser dar por simples constatação visual, já que não depende de análises contextuais.⁴⁴

39. Embora tenham sido apontados os dados relativos ao ano de 2021, os relatórios de transparência são emitidos desde 2012, isto é, em período anterior ao ajuizamento da ação judicial em comento.

40. X. *Transparency Reports*. Disponível em: <https://transparency.x.com/pt/reports/rules-enforcement.html#2021-jul-dec>, Acesso em: 22 abr. 2024.

41. *Idem*.

42. *Idem*.

43. No caso de direitos de autor ou direitos conexos, o §2º do art. 19 prevê que deverá ser aplicada a regra prevista em lei específica. A ausência de regramento específico, todavia, implica a prevalência da responsabilização do provedor a partir da simples notificação.

44. NITRINI, Rodrigo Vidal. *Liberdade de expressão nas redes sociais: o problema jurídico da remoção de conteúdo pelas plataformas*. (Doutorado) – Faculdade de Direito da Universidade de São Paulo, São Paulo, 2020, pág. 169. Disponível em: <https://www.teses.usp.br/teses/disponiveis/2/2134/tde->

O argumento mais sensível do acórdão se concentra na ideia de que a reserva de jurisdição conduz ao esvaziamento do “*direito básico de efetiva prevenção e reparação de danos patrimoniais e morais, individuais, coletivos e difusos*”. Com isso, os julgadores justificam que o provedor poderia ter adotado uma postura diligente para atender a pretensão autoral sem deixar de preservar a liberdade de expressão. Este parece ser o núcleo das principais críticas envolvendo o modelo de responsabilidade estabelecido no art. 19.

Nesta linha de raciocínio, Dantas e Neto argumentam que o pressuposto da judicialização para que se atribua responsabilidade civil ao provedor de aplicação constitui *obstáculo à defesa dos direitos de personalidade das potenciais vítimas*⁴⁵ Além disso, contrapõem que a intervenção do Judiciário *não parece contribuir para afastar o risco de censura ou de indevida intervenção estatal para a liberdade de expressão*⁴⁶.

Ao defender o regime de solidariedade *ex delicto*, Eduardo Tomasevicius justifica que “*esse sistema de proteção impõe o dever de vigilância dos provedores de aplicações de internet, ante a possibilidade de responder diretamente pelos atos dos usuários*”. Nesse sentido, conclui que o sistema adotado pelo Marco Civil consubstanciado na responsabilidade subsidiária dos provedores tende a facilitar a prática de delitos.⁴⁷

De forma convergente, Marcelo Bechara defende que o texto do art. 19 não é compatível com a efetiva proteção da dignidade da pessoa humana e que a necessidade da prestação jurisdicional adiciona uma camada de complexidade ao processo de moderação, podendo vir a “*permitir que conteúdos difamatórios ou abusivos permaneçam online por um período extenso, causando danos adicionais à reputação e à integridade emocional das pessoas afetadas*”⁴⁸

22032021-171558/pt-br.php. Acesso em: 25 mai. 2024.

45. DANTAS, Juliana de Oliveira Jota; MOTA NETO, Leonardo Lima. *Liberdade de expressão versus Responsabilidade dos provedores no marco civil da internet*. Revista da AGU, Brasília, v. 21, nº 04, p. 143-162, out./dez. 2022, pág. 153.

46. *Idem*.

47. TOMASEVICIUS FILHO, Eduardo. *Marco Civil da internet: uma lei sem conteúdo normativo*. Estudos Avançados. São Paulo: Direito GV, v. 30, n 86, pág. 269-285, abr. 2016, pág. 282.

48. HOBAlKA, Marcelo Bechara de Souza. *A lei do atrito e a inconstitucionalidade do art. 19 do Marco Civil da Internet*. In. JOTA. Disponível em <https://www.jota.info/opiniao-e-analise/artigos/a-lei-do-atrito-e-a-inconstitucionalidade-do-art-19-do-marco-civil-da-internet-17052024> . Acesso

Nota-se que há uma transposição do olhar para a condição da vítima, com o propósito de garantir a reparação econômica em face da lesão aos direitos da intimidade, vida privada, honra e imagem.

A preocupação em resguardar a reparação dos danos extrapatrimoniais atinentes ao usuário notificante é, evidentemente, legítima. Entretanto, parece ignorar os demais interesses em cena e, mais que isso, as consequências que podem se sobrepor a esta percepção unidimensional.

A relação jurídica, entretanto, envolve interesses, direitos e deveres que atingem quatro pólos distintos: a) a pessoa que promove as postagens na plataforma, b) os provedores de aplicação, c) os usuários que se sentem ofendidos com determinado conteúdo e d) os demais usuários que acessam a plataforma em busca dos conteúdos veiculados. Dessa forma, há que se reconhecer que há bens jurídicos constitucionalmente importantes e dignos de tutelas em todos os pólos dessa relação.⁴⁹

Na verdade, ao se decidir pela responsabilidade civil objetiva, inscrita no Código de Defesa do Consumidor, em detrimento da regra específica do Marco Civil, o Estado-juiz acaba concedendo ao provedor duas alternativas: suprimir o conteúdo tão logo recebe a notificação, seguindo a lógica do “*notice and take down*”, ou manter o conteúdo na plataforma por entender que não constitui risco a direito do notificante.⁵⁰

Considerando que o ente privado dificilmente atrairá para si um risco desta dimensão, o resultado prático é a transferência do controle prévio do conteúdo inserido pelos usuários ao provedor de aplicação. Com isso, o calibre entre os direitos da personalidade de liberdade de expressão ficará a cargo do ente privado.

Em adição, a plataforma se vê induzida a realizar o monitoramento de conteúdo movida pelo fator econômico, isto é, com o intuito de evitar eventual condenação indenizatória na esfera judicial, o que poderá prescindir da ponderação dos direitos fundamentais em conflito. De fato, a *abordagem mais cautelosa é agir de acordo com qualquer indicação de ilegalidade, sem se envolver em qualquer equilíbrio sofisticado*

em: 25 mai. 2024.

49. *Idem*.

50. SOUZA, Carlos Afonso Pereira de; LEMOS, Ronaldo. *Marco Civil da Internet: construção e aplicação*. Juiz de Fora: Editar, 2016, pág. 86.

de direitos em conflito.⁵¹

Dessa forma, o Poder Judiciário acaba concedendo, tacitamente, ao ente privado o poder de realizar o monitoramento de todo o conteúdo veiculado pelos usuários e, em última análise, de dizer o direito, outorgando poderes em favor do *tribunal das Big Techs*⁵². Isto é, colocam os intermediários em uma situação em que eles são essencialmente obrigados a decidir sobre direitos e interesses concorrentes.⁵³

Se pensarmos que os provedores de aplicação, com destaque para as redes sociais, se estruturaram como modelo de negócio a ganharam dimensão a partir da livre circulação de dados na rede, a atribuição de responsabilidade objetiva não possui apenas a face virtuosa da reparação civil e proteção dos direitos da personalidade. Paralelamente, se está a agigantar o poder das plataformas sobre os usuários e a facilitar arbitrariedades.

Nesse sentido, Carlos Affonso de Souza e Arnaldo Lemos ponderam que a atribuição do dever de avaliar se o conteúdo causa ou não dano à suposta vítima, pode resultar no *empoderamento dos provedores para decidir o que deve e o que não deve ser exibido mediante critérios que não são apenas aqueles constantes em seus termos de uso*⁵⁴.

De igual forma, alertam Teffé e Souza⁵⁵ que:

(...) eventual aumento desproporcional da responsabilidade das plataformas por conteúdos de terceiros poderia conduzir a um cenário de censura severa, no qual as plataformas preventivamente optariam por remover conteúdos e perfis controversos, os quais não necessariamente estariam causando danos a outrem. Fato esse que atingiria a liberdade de expressão e a

51. Tradução livre: “the most cautionary approach is to act upon any indication of illegality, without engaging in any sophisticated balancing of rights in conflict”. FROSIO, Giancarlo. *The Oxford Handbook of Online Intermediary Liability*. Oxford: Oxford University Press, 2020, pág. 527.

52. LEONARDO, Rodrigo Xavier. *Op. Cit.*

53. Tradução livre: “they place intermediaries in a situation where they are essentially required to decide about competing rights and interests”. FROSIO, Giancarlo. *The Oxford Handbook of Online Intermediary Liability*. Oxford: Oxford University Press, 2020, pág. 527.

54. SOUZA, Carlos Afonso Pereira de; LEMOS, Ronaldo. *Marco Civil da Internet: construção e aplicação*. Juiz de Fora: Editar, 2016, pág. 85.

55. TEFFÉ, Chiara Spadaccini de; SOUZA, Carlos Afonso. *Op. Cit.*

diversidade de opiniões na rede.

A lógica da prevenção de danos deve caminhar conjuntamente com a proteção das liberdades constitucionais, de forma que as imunidades e deveres sejam desenvolvidos criticamente a depender da gravidade dos riscos. A consideração sobre quais conteúdos ultrapassam ou não os limites da liberdade de expressão deve ser um processo, predominantemente, público e com discussões multisetoriais, e não um processo exclusivamente privado, conduzido por departamentos de plataformas digitais.

A atividade de moderação já é realizada pelos provedores por decorrência de seus próprios termos de uso, que lhes conferem amplo poder de regulação do discurso. Nesse sentido, as plataformas não são neutras e exercem julgamentos valorativos em sua atividade fim.

Na prática, estes agentes passam a atuar como *os novos governantes, construindo sistemas de governança semelhantes ao próprio sistema de justiça, em que os moderadores de conteúdos atuam numa capacidade muito semelhante à dos juízes*⁵⁶.

A criação do Conselho de Supervisão (*Oversight Board*) pela empresa Meta e Conselho Consultivo pela Google ilustram esse processo de mimetização do poder estatal. Embora essas estruturas simbólicas busquem incorporar valores públicos em suas atividades e implementar medidas de transparência e *accountability*, não necessariamente são capazes de sanar os déficits democráticos da moderação de conteúdo privada.

Em relação ao Conselho da Google, não é possível aferir em que medida a participação dos diversos atores sociais por meio das consultas públicas contribui para as deliberações internas⁵⁷.

O Conselho de Supervisão da Meta, por sua vez, apesar de ser composto por consultores independentes, possui atuação restrita à revisão das decisões de remoção de

56. KLONICK, Kate. *The New Governors: The People, Rules, and Processes Governing Online Speech*. HARVARD LAW REVIEW. 1598, 1647 (2018). Disponível em: The New Governors: The People, Rules, and Processes Governing Online Speech - Harvard Law Review. Acesso em: 15 jun. 2024.

57. MULLIGAN, Deirde, K.; BAMBERGER, Kenneth A. Allocating Responsibility in Content Moderation: A Functional Framework. *Berkeley Technology Law Journal*. Berkeley: University of California School of Law. v. 36, n. 03, p. 1091-1171, 2021. pág. 1173.

conteúdos específicos, o que limita o seu valor substantivo⁵⁸. Além disso, se as recomendações emitidas pelo Conselho sobre as políticas de conteúdo da empresa não são vinculativas⁵⁹, não se sabe se a atuação é apenas formal ou se há contribuição efetiva para o aprimoramento da política de moderação do provedor.

Passados, hoje, 10 (dez) anos da promulgação do Marco Civil, novas situações despontaram e a questão afeta à moderação de conteúdo veiculado na internet tomou novas proporções. De lá pra cá, episódios envolvendo a disseminação de *fake news* e discursos de ódio (*hate speech*), por exemplo, dimensionaram o problema e, inclusive, serviram de substrato para a elaboração do PL 2630/2020, que teve como propósito a regulação das plataformas de mídias sociais, incluindo medidas para a moderação de conteúdo. A tramitação do Projeto de Lei, todavia, foi paralisada por divergências na redação⁶⁰.

Em debate recente promovido pela Universidade de São Paulo, no seminário intitulado “Democracia e plataformas digitais”, a professora Laura Schertel afirmou que a discussão em torno do art. 19 é importante, pois, ao estabelecer a responsabilidade judicial pontual e posterior, entende que o Marco Civil deixa para as plataformas as grandes decisões sobre o conteúdo⁶¹.

Dando sequência à sua reflexão, acresce que é preciso pensar um modelo de regulação que esteja adequado às características da nova internet, com plataformas que

58. MULLIGAN, Deirde, K.; BAMBERGER, Kenneth A. Allocating Responsibility in Content Moderation: A Functional Framework. *Berkeley Technology Law Journal*. Berkeley: University of California School of Law. v. 36, n. 03, p. 1091-1171, 2021. pág. 1177-1178.

59. O item 7.3 do Estatuto do Conselho de Supervisão assim prevê: “Independent of any pending case, Facebook may request policy guidance from the board. This guidance may concern the clarification of a previous decision by the board or guidance on possible changes to Facebook’s content policies. All guidance will be Advisory”. Disponível em: https://about.fb.com/wp-content/uploads/2019/09/oversight_board_charter.pdf. Acesso em: 15 jun. 2024.

60. MACHADO, Caio Vieira. DURIGAN, Victor. PEREIRA, Laura. *PL das Fake News: entenda o que é, seu impacto e as principais críticas*. In JOTA. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/pl-das-fake-news-entenda-o-que-e-seu-impacto-e-as-principais-criticas-18042022#:~:text=O%20PL%20das%20Fake%20News,seja%20superior%20a%2010%20milh%C3%B5es.> . Acesso em: 27 mai. 2024.

61. MENDES, Laura Schertel. In. Seminário Democracia e Plataformas Digitais. Disponível em: <https://youtu.be/ANfK8RIY1ho> Acesso em: 24 mai. 2024.

não são neutras, cabendo ao Congresso dar os parâmetros a partir dos quais as decisões devem ser tomadas.⁶²

A Comissão de juristas responsável pela apresentação do anteprojeto de reforma do Código Civil, propôs em seu relatório final a revogação do art. 19 do Marco Civil, para introduzir *uma nova frente na regulação de conteúdo online pelas plataformas digitais*.⁶³

O professor Ricardo Campos, integrante da Subcomissão de Direito Digital, argumenta que o art. 19 é anacrônico e não condiz com a estrutura da internet, por isso mesmo, não reflete a agenda regulatória global. A proposta da Subcomissão segue no sentido de que os provedores devem assumir o *dever de curadoria do conteúdo que circula*⁶⁴, influenciada pela Lei de Serviços Digitais (Digital Services Act) da União Europeia.

A moderação de conteúdo constitui atividade complexa e qualquer intervenção, seja ela regulatória ou judicial, precisa considerar o atual momento social, em que os provedores de aplicações alçaram um patamar de importância outrora inimaginável, centrados no mercado da informação, aptos a influenciar pessoas, decidir quais informações chegam até elas, impondo padrões e opiniões, capazes de alterar substancialmente mercados e sociedades.

Embora haja um certo apelo para a ampliação da responsabilidade civil dos provedores de aplicação, principalmente diante do uso massivo das redes sociais, exemplos de provedores de aplicação, a declaração de inconstitucionalidade do art. 19 não parece ser a resposta. O descontentamento ou insuficiência do substrato normativo que rege a moderação de conteúdo deve ser suprido pela via legislativa e não judicial.

Caso a Suprema Corte chegue à conclusão de que o art. 19 é inconstitucional a fim de ampliar a responsabilidade atribuída aos provedores de aplicação, pode-se afirmar que teremos uma mudança de paradigma em relação ao próprio papel destes

62. *Idem*.

63. NUNES, Dierle. MACIEL, Mathaus Miranda. *Polêmico artigo 19 do Marco Civil da Internet e dilema da moderação de conteúdo*. In. CONJUR. Disponível em: <<https://www.conjur.com.br/2024-mai-11/o-polemico-artigo-19-do-marco-civil-da-internet-e-o-dilema-da-moderacao-de-conteudo/>>. Acesso em: 24 mai. 2024.

64. *Idem*.

agentes privados na sociedade.

No momento de escrita deste artigo, o Plenário do STF voltou a se reunir para decidir o tema e formou maioria pela inconstitucionalidade parcial do artigo 19 do Marco Civil da Internet, restando pendentes ainda votos e a publicação de acórdão a fim de definir qual seria a aplicabilidade do artigo 19 a partir do julgamento, e quais seriam, exatamente, os deveres de moderação de conteúdo exigidos das plataformas digitais⁶⁵.

4. A DISCUSSÃO DA CONSTITUCIONALIDADE DO ARTIGO 19 DO MARCO CIVIL DA INTERNET SOB A ÓTICA DA LIBERDADE DE EXPRESSÃO E OS RISCOS NO AUMENTO DO EXERCÍCIO DE PODER PELAS PLATAFORMAS DIGITAIS.

Como exposto, a defesa da liberdade de expressão tem surgido como principal tese defensiva das plataformas digitais para sustentar por uma aplicação literal do artigo 19 do Marco Civil, isentando-se, assim, da responsabilidade por conteúdos postados por seus usuários e impulsionados nas plataformas.

A liberdade de expressão é consagrada no Brasil na Constituição da República, por uma série de artigos, notadamente o art. 5º, inciso IV, que trata da *livre manifestação de pensamento, vedado o anonimato*; inciso VI, que trata da *liberdade de consciência e crença*; e inciso IX, que trata da *livre expressão intelectual, artística, científica e de comunicação, independente de censura*.

A tese da isenção de responsabilidade das plataformas digitais como defesa da liberdade de expressão tem sido defendida por diversas abordagens. Em “*The Reverse Spider-Man Principle: With Great Responsibility Comes Great Power*”, Eugene Volokh parte de uma perspectiva liberal e, de forma sintética, argumenta pela não responsabilização das plataformas digitais pela moderação de conteúdo *online*, partindo do princípio por ele chamado de “homem aranha reverso”, representado pela máxima de que “grandes responsabilidades atraem grandes poderes”.

65. BRASIL, Supremo Tribunal Federal. *STF define parâmetros para responsabilização de plataformas por conteúdos de terceiros*. 26 mai. 2025. Disponível em: <https://noticias.stf.jus.br/posts/noticias/stf-define-parametros-para-responsabilizacao-de-plataformas-por-conteudos-de-terceiros/>. Acesso em: 02 jul. 2025.

Em geral, Volokh argumenta, então, que a exigência de monitoramento abriria portas para que as empresas exercessem mais poder sobre seus consumidores⁶⁶:

Impor responsabilidade legal a tais empresas pode, assim, pressioná-las a exercer poder mesmo quando, de outra forma, não o fariam. E isso é verdade em certa medida mesmo que a responsabilidade seja aceita apenas como uma norma moral ampla, criada e reforçada pela pressão pública (provavelmente oriunda de setores influentes da sociedade, como a mídia, ativistas ou organizações profissionais), e não como uma norma legal. Essa norma moral aumentaria os custos compensatórios da falta de fiscalização. Ela diminuiria os custos da fiscalização: por exemplo, a norma e a pressão correspondente provavelmente atuariam sobre todos os principais concorrentes, de modo que as pressões competitivas normais, que incentivam uma atitude de "o cliente sempre tem razão", seriam drasticamente reduzidas. E, em algum momento, a norma poderia se tornar o padrão contra o qual a razoabilidade do comportamento é medida em termos legais. (...) Pode-se aprovar ou desaprovar o exercício de tal poder por grandes corporações empresariais sobre o discurso público; mas meu ponto aqui é simplesmente que os apelos por maior responsabilidade de fato aumentaram o exercício de tal poder.

Por fim, Volokh conclui com o argumento de que, com o *Big Data* e aumento da

66. Tradução dos Autores. "Imposing legal responsibility on such companies can thus pressure them to exercise power even when they otherwise wouldn't have. And that is so in some measure even if responsibility is accepted just as a broad moral norm, created and enforced by public pressure (likely stemming from influential sectors of society, such as the media or activists or professional organizations), and not a legal norm. That moral norm would increase the countervailing costs of non-policing. It would decrease the costs of policing: For instance, the norm and the corresponding pressure would likely act on all major competitors, so the normal competitive pressures encouraging a "the customer is always right" attitude would be sharply reduced. And at some point, the norm might become the standard against which the reasonableness of behavior is measured as a legal matter.(...) One might approve or disapprove of such power exercised by large business corporations over public discourse; but my point here is simply that calls for great responsibility have indeed increased the exercise of such power." VOLOKH, Eugene. *The Reverse Spider-Man Principle: With Great Responsibility Comes Great Power*. Journal of Free Speech Law. Los Angeles: Journal of Free Speech Law. v. 03, n. 01, p. 197-216, 2023.

capacidade de monitoramento das plataformas digitais, caso estas sejam responsabilizadas indefinidamente pelos atos de seus clientes, isto levaria a uma tendência de que elas, de fato, passariam a exercer este poder⁶⁷.

Contudo, também há críticos desta abordagem. Evelyn Douek, em artigo publicado na Harvard Law Review, apresenta uma visão crítica da discussão em torno do tema da moderação de conteúdo nas plataformas digitais. Segundo a autora, o “estado da arte” da discussão envolvendo a moderação de conteúdo trata a moderação como uma transposição da lógica *offline* para o mundo *online*. Isto é: a moderação pensada e discutida pela maior parte dos legisladores, tribunais e juristas, hoje, é baseada em casos individuais e numa visão processualista da moderação, ou seja, pela qual a moderação passaria por um processo similar ao processo judicial, com contraditório e decisão pela parte moderadora.

Esta transposição, segundo a autora, seria uma transposição da discussão envolvendo a liberdade de expressão (*free speech*) e a Primeira Emenda⁶⁸ para o contexto digital. Neste contexto, as plataformas frequentemente são vistas como um *novo governo*⁶⁹, responsável por implementar regras materiais e processuais de controle de conteúdo.

Ocorre que, segundo a autora, esta visão tradicional sobre a moderação de conteúdo tem pontos cegos, que leva a más proposições políticas de solução dos problemas envolvendo o tema. Por exemplo, em geral, na prática, a moderação de conteúdo se dá por diversas formas mais amplas do que a análise individualizada de conteúdos, como: a proibição de *spam*, proibição de contas falsas e certos usos de *bot*, a busca automatizada, a terceirização para empresas subcontratadas, *trade-offs* envolvendo

67. *Idem*.

68. “First Amendment. Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.” WIKIPEDIA. *Primeira Emenda à Constituição dos Estados Unidos*. Disponível em: <https://pt.wikipedia.org/wiki/Primeira_Emenda_%C3%A0_Constitui%C3%A7%C3%A3o_dos_Estados_Unidos#:~:text=A%20%22Primeira%20Emenda%22%20foi%20adotada,de%20infringir%20seis%20direitos%20fundamentais.>> Acesso em: 03 jul. 2024.

69. DOUEK, Evelyn. Content Moderation as Systems Thinking. Harvard Law Review. Cambridge: Harvard University Press. v. 136, n. 02, p. 526-607, Dec. 2022, pág. 529.

falsos positivos e falsos negativos, dentre outros.

A "moderação de conteúdo," especialmente, mas não exclusivamente, nas maiores plataformas, agora inclui muito mais coisas do que incluía há alguns anos: maior dependência de moderação automatizada; colocação de rótulos em postagens; parcerias com verificadores de fatos; maior colaboração entre plataformas e governo; aumento da dificuldade para os usuários compartilharem conteúdo; fornecimento de recursos para os usuários controlarem sua própria experiência online; análise além do conteúdo das postagens para como os usuários se comportam online, a fim de determinar o que deve ser removido; e ajustes nas dinâmicas subjacentes das próprias plataformas. As pessoas e os processos que determinam como o conteúdo gerado pelos usuários é tratado nas plataformas online são, portanto, muito mais heterogêneos do que descrito na visão padrão. Moderadores de conteúdo incluem engenheiros, gerentes de produto, autoridades fora das plataformas, equipes que monitoram sinais comportamentais, pares da indústria e parceiros governamentais. Em suma, a moderação de conteúdo é um sistema complexo e dinâmico, grande parte do qual não será examinada se o foco estiver na revisão de casos individuais em vez de seu contexto institucional e inter-relações.⁷⁰

Além disso, este cenário cria a exigência, para as plataformas digitais, para que

70. Tradução dos autores. "Content moderation," especially but not exclusively at the largest platforms, now includes many more things than it did even a few years ago: increased reliance on automated moderation; sticking labels on posts; partnerships with fact-checkers; greater platform and government collaboration; adding friction to how users share content; giving users affordances to control their own online experience; looking beyond the content of posts to how users *behave* online to determine what should be removed; and tinkering with the underlying dynamics of the very platforms themselves. The people and processes that determine how user-generated content is treated on online platforms are therefore far more heterogeneous than depicted in the standard account. Content moderators include engineers, product managers, authorities outside platforms, teams monitoring behavioral signals, industry peers, and government partners. In short, content moderation is a complex and dynamic system, much of which will not be examined if the focus is on reviewing individual cases rather than their institutional context and inter-relationships."DOUEK, Evelyn. Content Moderation as Systems Thinking. Harvard Law Review. Cambridge: Harvard University Press. v. 136, n. 02, p. 526-607, Dec. 2022. pág. 531.

concedam direitos processuais aos seus usuários, uma vez que estes são garantidos no mundo offline e, em geral, pelas constituições. A autora faz uma afirmação que corrobora a tese de Eugene Volokh no sentido de que, caso as plataformas tenham poderes para moderar conteúdo, elas vão, certamente, usar esses poderes além da Lei:

Os reguladores recorrem aos procedimentos das plataformas porque limitações constitucionais e práticas ao poder governamental significam que a tarefa de estabelecer a maioria das regras substantivas de moderação de conteúdo não pode ser retirada das empresas privadas. As plataformas podem e irão se envolver em moderação de conteúdo além do que a lei poderia prescrever.⁷¹

Além disso, a autora faz uma interessante constatação: o Estado não tem condições práticas de substituir as plataformas no papel de moderar o conteúdo existente dentro delas mesmas⁷². Dessa forma, segundo a autora, os reguladores estão corretos em focar no *processo* de moderação e não no *conteúdo* a ser regulado, mas a abordagem em casos individuais é equivocada⁷³.

Considerando estes pontos, observa-se as vantagens da tese defendida por Douek, para que a sociedade adote uma *segunda onda* das propostas de regulação de moderação de conteúdo, baseado em *sistemas de moderação*, e não em moderação de conteúdo de casos individualizados, tendo em vista a escala, velocidade e precisão exigidas para a regulação do tema. Neste cenário, os provedores de aplicação deveriam ser responsabilizados por criar *sistemas ex ante* de regulação, e responder pelo funcionamento desses sistemas, mas não responder apenas *ex post* pela correção de casos individualizados. Esta seria uma abordagem anti-perfeccionista, prática e que tiraria o foco do debate sobre a liberdade de expressão.

71. Tradução dos Autores. “Regulators turn to platform procedure because constitutional and practical limitations on governmental power mean that the job of setting most substantive content moderation rules cannot be taken away from private companies. Platforms can and will engage in content moderation beyond what the law could proscribe” DOUEK, Evelyn. *Op. Cit.* pág. 531.

72. “This is a descriptive, not normative, observation: the state simply does not have the capacity to usurp platforms as the frontline of content moderation.” DOUEK, Evelyn. *Op. Cit.* p. 532.

73. *Idem.*

5. CONCLUSÃO

A questão relacionada à moderação de conteúdo no Brasil tomou novos rumos diante da afetação dos REs nºs 1.067.258 e 1.037.396 pela sistemática de repercussão geral, que segue pendente de julgamento no Supremo Tribunal Federal, no entanto, com maioria já formada para se declarar uma inconstitucionalidade parcial do artigo 19 do Marco Civil.

A matéria controvertida no segundo caso diz respeito a constitucionalidade do art. 19 do Marco Civil da Internet que definiu um regime de responsabilidade subjetiva para os provedores de aplicação ao privilegiar a reserva de jurisdição para a moderação de conteúdo veiculado *online*.

Muito embora exista um apelo à ampliação da responsabilidade civil dos provedores de aplicação por conteúdos veiculados por terceiros, a questão deve ser avaliada com cautela. Como visto, estes provedores já adotam uma postura ativa na moderação de conteúdo *online* em virtude dos seus termos de uso, todavia, suprimir o filtro judicial e transpor para as mãos do ente privado a responsabilidade pelo exercício desta atividade, implica aumentar significativamente o poder que estes agentes exercem sobre nós.

Contudo, como demonstramos neste estudo, embora a regulação das Plataformas Digitais, em geral, e os Temas 533 e 987 no STF passem por diversos debates de grande complexidade, a defesa da liberdade de expressão tem sido utilizada muitas vezes como um argumento espantalho pelos defensores da não regulação.

Contudo, focar apenas neste ponto do debate é insuficiente para se pensar a regulação das Plataformas. As questões de direitos dos consumidores (usuários), mercados concorrenciais, democracia, e os próprios limites ao exercício da liberdade de expressão devem ser considerados. Não é possível responder aos dilemas existentes a partir de aportes exclusivamente técnicos, tampouco idealistas.

Responder à questão “quem são os intermediários” da internet é necessário. Neste sentido, tanto do art. 19 do Marco Civil da Internet, quanto do 260 DSA estadounidense, dizem respeito a uma internet que não existe mais, em que os provedores de serviços na Internet atuavam muito mais como intermediários de fato, disponibilizando espaços para publicação genuína de seus usuários. Exemplos claros e bem lembrados disso são o Orkut, os blogs etc.

A internet de hoje é dominada pelas maiores empresas de mídia do mundo, cujo modelo de negócios consiste na *clusterização* e outras formas de tratamento de dados de seus usuários, para venda para anunciantes. Nesse modelo de negócios, as plataformas lucram com o engajamento acima de tudo, mesmo que este engajamento se dê a partir de conteúdos ilegais.

Não obstante, as plataformas lucram com o impulsionamento de *fake news*, opiniões políticas e desafiam a democracia como já amplamente comprovado. Contrapor a necessidade de regulação dessas plataformas única e exclusivamente à liberdade de expressão não pode ser, para os juristas, um impasse no debate. Pelo contrário, é preciso abraçar o desafio de continuar estudando o tema profundamente a fim de encontrar soluções adequadas.

Nesse sentido, a declaração de inconstitucionalidade do art. 19 do Marco Civil da Internet não parece ser o caminho mais acertado, embora o STF, até o momento de escrita deste artigo, venha decidindo por sua inconstitucionalidade parcial. Seja porque o regime nele definido se alinha aos princípios constitucionais, seja porque se estabelecerá um novo paradigma social em que os provedores de aplicação passarão a exercer poderes de vigilância muito semelhantes aos poderes de polícia. Por outro lado, não há dúvidas que este dispositivo legal deve ser interpretado em consonância com o restante do ordenamento jurídico para que não se permita a terceirização das responsabilidades, nem tampouco a crença que as Plataformas são absolutamente neutras, como já ficou claro em diversos casos.

REFERÊNCIAS

- BRASIL. Câmara dos Deputados. *Projeto de Lei nº 2.630/2020*. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2256735>. Acesso em: 17 jun. 2024.
- BRASIL. Superior Tribunal de Justiça. *Recurso Especial n. 1.501.603 - RN (2014/0290071-6)*. Relatora: Min. Nancy Andrighi. Dezembro de 2017. Disponível em: <https://processo.stj.jus.br/processo/pesquisa/?aplicacao=processos.ea&tipoPesquisa=tipoPesquisaGenerica&termo=REsp%201501603>. Acesso em 26 jun. 2024.
- BRASIL. Superior Tribunal de Justiça. *Recurso Especial n. 1.512.647-MG*. Rel. Min. Luís Felipe Salomão. DJe 15 ago. 2015. Disponível em

[https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ATC&seque-
cial=45693836&num_registro=201301628832&data=20150805&tipo=91&formato=PDF](https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ATC&seque-
cial=45693836&num_registro=201301628832&data=20150805&tipo=91&formato=PDF).

Acesso em: 26 jun. 2024.

BRASIL. *Resolução CGI.br/RES/2009/003/P*. Disponível em: <[https://www.cgi.br/resolucoes/docu-
mento/2009/003](https://www.cgi.br/resolucoes/docu-
mento/2009/003)>. Acesso em: 26 jun. 2024.

BRASIL. Lei n 12.965, 23 de abril de 2014. *Marco civil da internet*. Brasília, DF: Presidência da Repú-
blica, 2018. Disponível em [http://www.planalto.gov.br/ccivil_03/_ato2011-
2014/2014/lei/l12965.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-
2014/2014/lei/l12965.htm). Acesso em: 25 mai. 2024.

BRASIL, Senado Federal. *Projeto de Lei n. 232, de 2017*. Disponível em: [https://www25.se-
nado.leg.br/web/atividade/materias/-/materia/130820](https://www25.se-
nado.leg.br/web/atividade/materias/-/materia/130820). Acesso em: 28 jun. 2024.

BRASIL. Supremo Tribunal Federal. STF. *Inquérito 4.957*. Rel. Min. Alexandre de Moraes. Disponível
em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=6893258>. Acesso em: 17 jun. 2024.

BRASIL. Supremo Tribunal Federal. *Recurso extraordinário: 1.037.396/SP*. Relator: Min. Dias Toffoli.
Tema 987 – Repercussão Geral. Brasília, DF, DJe: 05 de abril de 2017. Disponível em:
[https://www.stf.jus.br/portal/jurisprudenciaRepercussao/verAndamentoProcesso.asp?inci-
dente=5160549&numeroProcesso=1037396&classeProcesso=RE&numeroTema=987](https://www.stf.jus.br/portal/jurisprudenciaRepercussao/verAndamentoProcesso.asp?inci-
dente=5160549&numeroProcesso=1037396&classeProcesso=RE&numeroTema=987) Acesso:
em 26 mai. 2024.

BRASIL. Supremo Tribunal Federal. *Recurso extraordinário: 1.057.258/MG*. Relator: Min. Luiz Fux.
Tema 533 - Repercussão geral. Brasília, DF, DJe: 27 junho de 2017. Disponível em:
[https://https://www.stf.jus.br/portal/jurisprudenciaRepercussao/verAndamentoPro-
cesso.asp?incidente=5217273&numeroProcesso=1057258&classeProcesso=RE&numero-
Tema=533](https://https://www.stf.jus.br/portal/jurisprudenciaRepercussao/verAndamentoPro-
cesso.asp?incidente=5217273&numeroProcesso=1057258&classeProcesso=RE&numero-
Tema=533) Acesso em: 26 mai. 2024.

BRASIL, Supremo Tribunal Federal. *STF define parâmetros para responsabilização de plataformas por
conteúdos de terceiros*. 26 mai. 2025. Disponível em: [https://noticias.stf.jus.br/postsnoticias/stf-
define-parametros-para-responsabilizacao-de-plataformas-por-conteudos-de-terceiros/](https://noticias.stf.jus.br/postsnoticias/stf-
define-parametros-para-responsabilizacao-de-plataformas-por-conteudos-de-terceiros/). Acesso
em: 02 jul. 2025.

BREGA, Gabriel Ribeiro. *A regulação de conteúdo nas redes sociais: uma breve análise comparativa
entre o NetzDG e a solução brasileira*. Revista Direito GV, São Paulo, v. 19, e2305, 2023.
<https://doi.org/10.1590/2317-6172202305>. Acesso em: 26 jun. 2024.

CASTELLS, Manuel; CARDOSO, Gustavo (Orgs.). *A Sociedade em Rede: do conhecimento à ação po-
lítica*; Conferência. Belém (Por): Imprensa Nacional, 2005.

DANTAS, Juliana de Oliveira Jota; MOTA NETO, Leonardo Lima. *Liberdade de Expressão versus Res-
ponsabilidade dos Provedores no Marco Civil da Internet*. Revista da AGU, Brasília, v. 21, n.º 04, p.
143-162, out./dez. 2022.

DOUEK, Evelyn. *Content Moderation as Systems Thinking*. Harvard Law Review. Cambridge: Har-
vard University Press. v. 136, n. 02, p. 526-607, Dec. 2022.

- FRAZÃO, Ana. *Plataformas digitais e os desafios para sua regulação jurídica*. In.: Direito, Tecnologia e Inovação. Belo Horizonte: Editora D'Plácido, 2018.
- FROSIO, Giancarlo. *The Oxford Handbook of Online Intermediary Liability*. Oxford: Oxford University Press, 2020.
- HOBAIKA, Marcelo Bechara de Souza. A lei do atrito e a inconstitucionalidade do art. 19 do Marco Civil da Internet. In. JOTA. Disponível em <https://www.jota.info/opiniao-e-analise/artigos/a-lei-do-atrito-e-a-inconstitucionalidade-do-art-19-do-marco-civil-da-internet-17052024>. Acesso em: 25 mai. 2024.
- JOBIM, Nelson. LEMOS, Renato. PARECER. In. CONJUR. Recurso Extraordinário questiona Marco Civil da Internet no STF. 9 dez. 2019. Disponível em: <https://www.conjur.com.br/wp-content/uploads/2023/09/clique-aqui-ler-parecer-ronaldo-lemos.pdf>. Acesso em: 25 jun. 2024.
- KLONICK, Kate. *The new governors: the people, rules, and processes governing online speech*. Harvard Law Review, v. 131, n. 1598, p. 1598-1670.
- LEONARDO, Rodrigo Xavier. Controle de constitucionalidade do Marco Civil da Internet em audiência no STF. In CONJUR. 3 abr. 2023. Disponível em: <https://www.conjur.com.br/2023-abr-03/direito-civil-atual-audiencia-publica-stf-controle-constitucionalidade-marco-civil-internet/>. Acesso em: 28 mai. 2024.
- MACHADO, Caio Vieira. DURIGAN, Victor. PEREIRA, Laura. PL das Fake News: entenda o que é, seu impacto e as principais críticas. In JOTA. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/pl-das-fake-news-entenda-o-que-e-seu-impacto-e-as-principais-criticas-18042022#:~:text=O%20PL%20das%20Fake%20News,seja%20superior%20a%2010%20milh%C3%B5es>. Acesso em: 27 mai. 2024.
- MENDES, Laura Schertel. In. Seminário Democracia e Plataformas Digitais. Disponível em: <https://youtu.be/ANfK8RIY1ho>. Acesso em: 24 mai. 2024.
- MULLIGAN, Deirde. K.; BAMBERGUER, Kenneth A. *Allocating responsibility in Content Moderation: A Functional Framework*. Berkeley Technology Law Journal. Berkeley University of California School of Law. v. 36, n. 03, p. 1091-1071, 2021.
- NITRINI, Rodrigo Vidal. *Liberdade de expressão nas redes sociais: o problema jurídico da remoção de conteúdo pelas plataformas*. (Doutorado) – Faculdade de Direito da Universidade de São Paulo, São Paulo, 2020.
- NUNES, Dierle. MACIEL, Matheus Miranda. Polêmico artigo 19 do Marco Civil da Internet e dilema da moderação de conteúdo. In. CONJUR. Disponível em: <https://www.conjur.com.br/2024-mai-11/o-polemico-artigo-19-do-marco-civil-da-internet-e-o-dilema-da-moderacao-de-conteudo/>. Acesso em: 24 mai. 2024.
- SALDÍAS, Osvaldo. *Coded for Export! The Contextual Dimension of the Brazilian Marco Civil da Internet*. Alexander von Humboldt Discussion Paper 2014-06. p. 01-24, nov. 2014.

SOUZA, Carlos Affonso Pereira de; LEMOS, Ronaldo. *Marco Civil da Internet: Construção e Aplicação*. Juiz de Fora: Editar, 2016.

TEFFÉ, C. S.; SOUZA, C. A. *Responsabilidade civil de provedores na rede: análise da aplicação do Marco Civil da Internet pelo Superior Tribunal de Justiça*. Revista IBERC, Belo Horizonte, v. 1, n. 1, p. 1–28, 2019. DOI: 10.37963/iberc.v1i1.6. Disponível em: <https://revistaiberc.emnuvens.com.br/iberc/article/view/6>. Acesso em: 26 jun. 2024.

TOMASEVICIUS FILHO, Eduardo. *Marco civil da internet: uma lei sem conteúdo normativo*. Estudos Avançados. São Paulo: Direito GV, v. 30, n. 86, p. 269-285, abr. 2016.

VOLOKH, Eugene. *The Reverse Spider-Man Principle: With Great Responsibility Comes Great Power*. Journal of Free Speech Law. Los Angeles: Journal of Free Speech Law. v. 03, n. 01, p. 197-216, 2023.

X. Transparency Reports. Disponível em: <https://transparency.x.com/pt/reports/rules-enforcement.html#2021-jul-dec>. Acesso em: 22 abr. 2024.