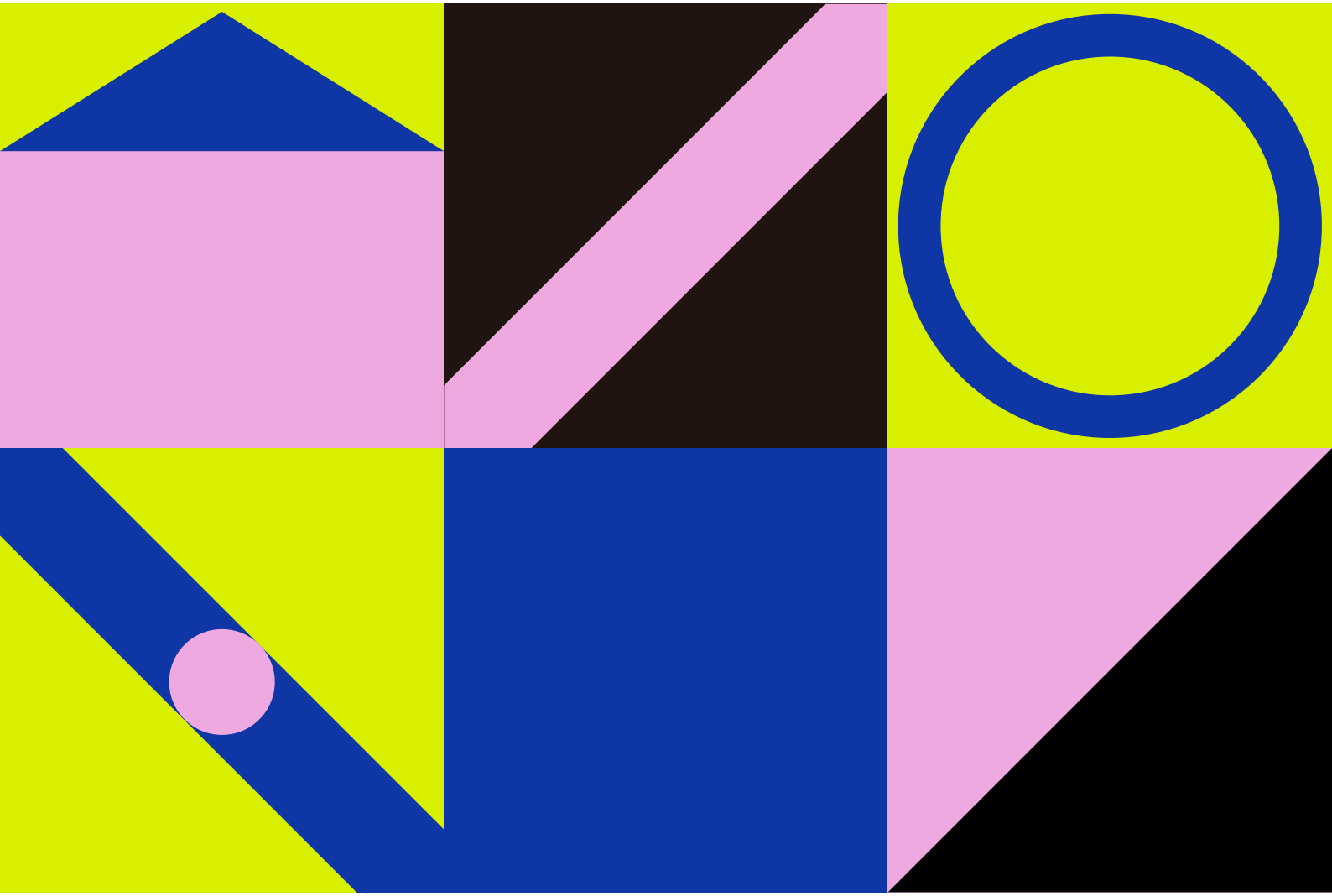
Instituto de
Pesquisa em
Direito & Tecnologia
do Recife



RELATÓRIO AMOSTRAL (NORTE-SUL GLOBAL) **DE CONCEITOS RELATIVOS À** RESPONSABILIDADE CIVIL DE INTERMEDIÁRIOS NA INTERNET - VOLUME 2

(AUSTRÁLIA - CANADÁ – INDONÉSIA - RÚSSIA)

Responsabilidade Civil

RELATÓRIO AMOSTRAL (NORTE-SUL GLOBAL) **DE CONCEITOS RELATIVOS À** RESPONSABILIDADE CIVIL DE INTERMEDIÁRIOS NA INTERNET - VOLUME 2

(AUSTRÁLIA - CANADÁ – INDONÉSIA - RÚSSIA)

Realização:
Instituto de Pesquisa em Direito
e Tecnologia do Recife - IP.Rec

Financiamento:
GOOGLE BRASIL

Pesquisa e texto:
André Lucas Fernandes
Danielle Novaes de Siqueira Valverde
Isabel Meira Constant
Lucas Santana da Silva
Rhaiana Caminha Valois

Revisão de conteúdo:
André Lucas Fernandes
Raquel Lima Saraiva.

Revisão geral (grafia, referências, normas técnicas):
Lucas Santana da Silva

Projeto gráfico:
Maria Clara Guimarães

Dados Internacionais de Catalogação na Publicação (CIP) (Câmara Brasileira do Livro, SP, Brasil)

Relatório amostral (norte-sul global) de conceitos relativos à responsabilidade civil de intermediários na internet : volume 2 [livro eletrônico] :

(Austrália - Canadá – Indonésia - Rússia) / André Lucas Fernandes...[et al.].-- 1. ed. -- Recife, PE : IP.rec, 2023.
PDF

Outros autores: Danielle Novaes de Siqueira Valverde, Isabel Meira Constant, Lucas Santana da Silva, Rhaiana Caminha Valois

Bibliografia.
ISBN 978-65-995947-6-2

1. Direito civil 2. Direito comparado 3. Internet
4. Responsabilidade civil I. Fernandes, André Lucas.
II. Valverde, Danielle Novaes de Siqueira.
III. Constant, Isabel Meira. IV. Silva, Lucas Santana da. V. Valois, Rhaiana Caminha.

23-148353 CDU-340.5

Índices para catálogo sistemático:

1. Direito comparado 340.5

Eliane de Freitas Leite - Bibliotecária - CRB 8/8415

RESUMO EXECUTIVO

Modelos de responsabilidade civil de intermediários tecnológicos, abordados sob a perspectiva histórico-conceitual, vêm sendo o cerne de um dos projetos de pesquisa conduzidos pelo IP.rec, desde o ano de 2021. Ao longo desse período, vários levantamentos bibliográficos foram realizados, entrevistas com especialistas foram conduzidas e materiais publicados. O primeiro Relatório abrange cinco países, distribuídos conforme pertençam ao Norte ou ao Sul Global. Pelo Norte Global, foram explorados a Alemanha, os Estados Unidos da América; do Sul Global, Brasil, Índia e México.

Esse segundo Relatório amplia o rol de países pesquisados, trazendo importantes referências na continuidade do processo de construção de conhecimento sobre o tema. O presente trabalho baseia-se na análise da evolução dos conceitos, considerando o contexto histórico em que surgiram, o que contribui para identificar os pressupostos comuns e conjecturar tendências de novos requisitos para o futuro. A Austrália e o Canadá representam o Norte Global, enquanto a Indonésia e a Federação Russa, o Sul Global.

Os Estados Unidos da América foram os primeiros a regular a responsabilidade civil dos provedores de serviço por danos decorrentes de conteúdo publicado por terceiros. Eles o fizeram ainda na década de 1990, quando a Internet comercial dava os seus primeiros passos. Mas foi durante as duas primeiras décadas do século XXI que se intensificaram as iniciativas regulatórias sobre a matéria. O Brasil, por exemplo, pacificou a questão em 2014, com o Marco Civil da Internet.

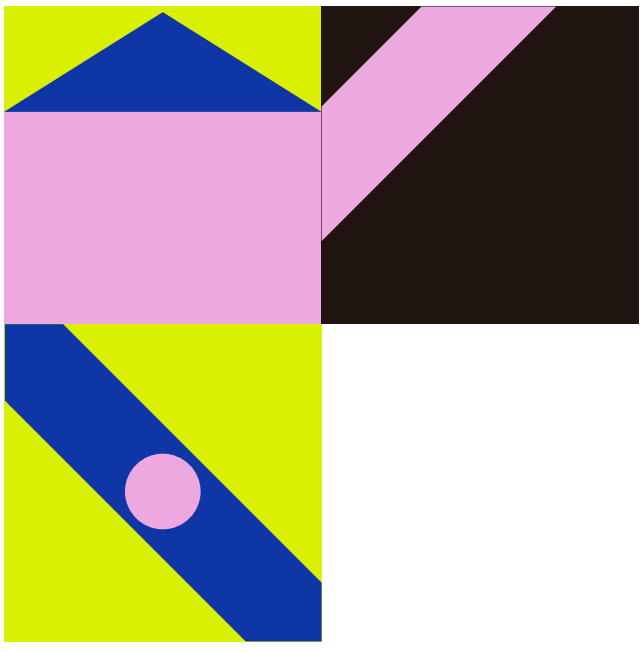
Dentre os países estudados, a Austrália regulamenta as hipóteses de incidência em diversos diplomas legais, de acordo com a natureza da matéria disciplinada, seja direitos autorais, direitos do consumidor ou proteção à violência contra menores. Em geral, segue o modelo *Notice and Takedown*, segundo o qual o provedor de aplicação será responsabilizado caso, tomando conhecimento da ilicitude do material publicado, deixe de adotar providências para excluí-lo ou bloqueá-lo, independentemente do grau de culpa do provedor. Nos últimos anos, várias leis foram aprovadas para tornar mais rígidos os critérios de remoção de conteúdo e aumentar o vigilantismo no país, enfraquecendo a criptografia e gerando prejuízos para a liberdade de expressão no país.

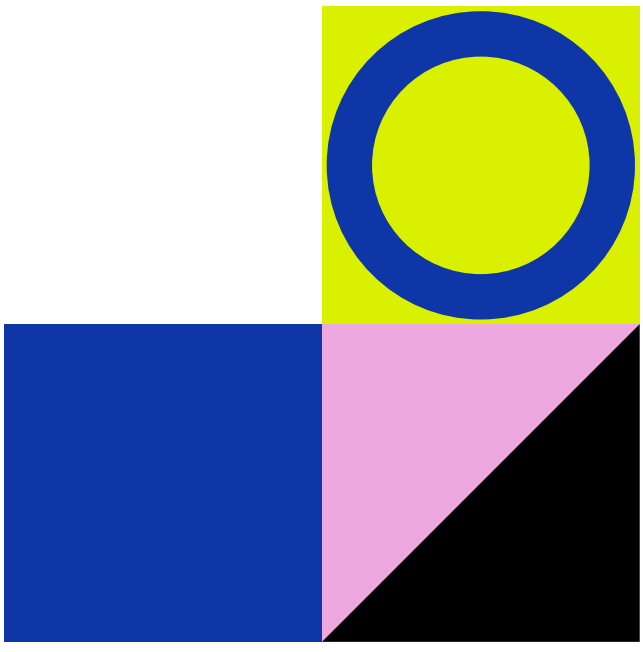
No Canadá, provedores de aplicação podem ser responsabilizados por conteúdos difamatórios, uma vez que a difamação é conduta tipificada como crime no código penal do país. Também podem ser responsabilizados com base na Lei de Direitos Autorais do país, considerando a propriedade intelectual do conteúdo publicado. Não existe no país, porém, legislação específica que abranja o conceito e as consequências civis para a responsabilidade de provedores de aplicação por danos decorrentes de conteúdo postado por terceiros - seus usuários. Contudo, há projetos de lei nesse sentido e precedentes abertos por jurisprudências que se baseiam na Lei de Direitos Autorais, na Lei de Modernização de Direitos Autorais e no Código Penal.

Os países do Sul Global analisados neste relatório apresentam modelos com características semelhantes, no que concerne à instrumentalização jurídica do Estado com o intuito de possibilitar-lhe o controle sobre o discurso e a expressão do pensamento, nas mídias de massa e no ambiente da Internet, sendo mais evidente na Federação Russa que, desde 2022, protagoniza invasão à Ucrânia. Ainda, esses países penalizam, duramente, os intermediários de informações e pessoas físicas, sejam usuários ou representantes de empresas de tecnologia da Informação, ao descumprirem obrigações legais. Em flagrante violação a direitos fundamentais, medidas estabelecidas facilitam a perseguição sistemática a opositores políticos, a jornalistas e suas fontes, além de cidadãos que retransmitem informações ilícitas ou antipáticas ao Governo.

Finalmente, numa perspectiva global, observa-se que os modelos de responsabilidade civil de intermediários tecnológicos são delineados conforme o regime político, sistema econômico, valores, cultura locais e anseios da sociedade, tendo como um de seus principais atores grandes empresas multinacionais de tecnologia que processam dados na Internet, onde as fronteiras terrestres se apresentam, cada vez mais, como desafios que implicam na adoção de novos programas de *compliance*, dos quais se espera, sempre, que sejam moldados em respeito aos direitos humanos.

Palavras-chaves: história dos conceitos; Internet; responsabilidade de intermediários; modelos de regulação; legislação comparada.





EXECUTIVE SUMMARY:

Models of civil liability of technological intermediaries approached from a historical-conceptual perspective have been the core of a research project conducted by IP.rec, since 2021. During this period, several bibliographical surveys were carried out, interviews with experts were conducted and materials were published. The materials cover five countries distributed according to whether they belong to the Global North or the Global South. For the North-Global, Germany, and the United States were explored, and Brazil, India and Mexico from the Global South.

This second Report expands the list of countries surveyed, bringing important references for building knowledge on the subject. The present work was based on analyzing the evolution of concepts considering the historical context in which they emerged, which helps to identify common assumptions and conjecture trends of new requirements for the future. Australia and Canada represent the Global North, while Indonesia and the Russian Federation represent the Global South.

The United States of America was the first to regulate the civil liability of service providers for damages resulting from content published by third parties. They did so in the 1990s, when the commercial Internet took its first steps. But it was during the first two decades of the 21st century that regulatory initiatives intensified. Brazil, for example, pacified the issue in 2014, with the Marco Civil da Internet.

Among the countries studied, Australia regulates the hypotheses of incidence in several legal diplomas, according to the nature of the disciplined matter, be it copyright, consumer rights or protection against violence against minors. In general, it follows the Notice and Takedown model, according to which the application provider will be held liable if, upon becoming aware of the published material's illegality, it fails to delete or block it, regardless of the provider's degree of fault. In recent years, several laws have been passed to tighten content removal criteria and increase vigilantism in the country, weakening encryption and harming freedom of expression.

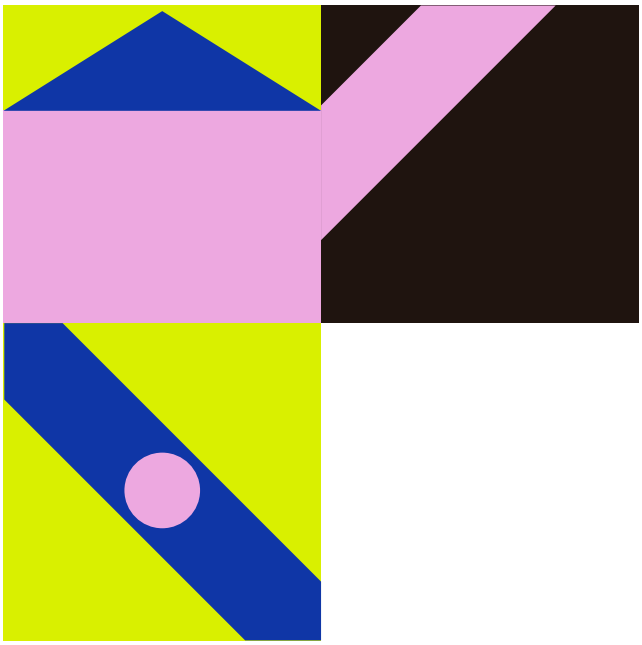
In Canada, application providers can be held liable for defamatory content, as defamation is a criminal offense under the country's penal code. They can also be held responsible based on the country's Copyright Law, considering the intellectual property of the published content. However, no specific legislation in the country covers the concept and civil consequences for the liability of application providers for damages resulting from content posted by third parties - their users. However, there are bills in this regard and precedents opened by jurisprudence based on the Copyright Act, the Copyright Modernization Act and the Canadian Penal Code.

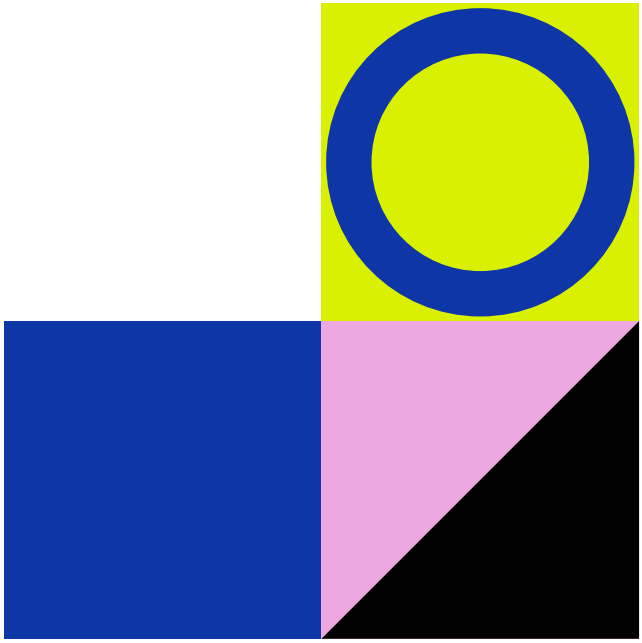
The countries of the Global South analyzed in this report present models with similar characteristics concerning the legal instrumentalization of the State to enable control over discourses and expressions in the mass media and in the Internet environment. The countries severely penalize information intermediaries and

individuals, whether users or representatives of information technology companies, when they fail to comply with legal obligations. In flagrant violation of fundamental rights, the established measures facilitate the systematic persecution of political opponents, journalists and their sources, and citizens who only pass on information that displeases the Government.

Finally, from a global perspective, it is observed that the models of civil liability of technological intermediaries are outlined according to the political regime, economic system, values, local culture and aspirations of society, having as one of its main actors multinational technology companies that process data on the Internet, where land borders increasingly present themselves as challenges that imply the adoption of new compliance programs, which are always expected to be shaped in respect of the human rights.

Keywords: history of concepts; Internet; intermediaries liability; regulation models; comparative legislation.





Sumário

LISTA DE SIGLAS E ABREVIATURAS

ACMA - Autoridade Australiana de Comunicações e Mídia

BESO - Basic Expectations of Online Safety

BSA - Broadcasting Services Act

ccTLD - country code Top-Level Domain

CIS - Stanford - The Center for Internet and Society - Stanford University

CRTC - Canadian Radio-Television and Telecommunications Commission.

CSP - Carriage Service Provider

Cth - Commonwealth

DMCA - Digital Millennium Copyright Act

IP.rec - Instituto de Pesquisa em Direito e Tecnologia do Recife

ICH - Internet Content Host

ISP - Internet service provider

LGBT - Lésbicas, Gays, Bissexuais e Transgênero

Kominfo - Ministério de Comunicação e Tecnologia da Informação

OCSP - Online Communication Service Provider

ONG - Organização Não Governamental

ONU - Organização da Nações Unidas

OSE Privado - Operadores de Sistemas Eletrônicos Privados

RKN - Roskomnadzor

TIC - Tecnologias da Informação e Comunicação

UDA - Uniform Defamation Acts

INTRODUÇÃO

O presente estudo é continuidade ao **RELATÓRIO AMOSTRAL (NORTE-SUL GLOBAL) DE CONCEITOS RELATIVOS À RESPONSABILIDADE CIVIL DE INTERMEDIÁRIOS NA INTERNET** (Alemanha, Espanha, Estados Unidos da América, Brasil, Índia e México), publicado pelo IP.rec - Instituto de Pesquisa em Direito e Tecnologia do Recife, no ano de 2021.

Trata-se de um dos produtos do projeto de pesquisa **Responsabilidade Civil de Intermediários: passado de experiência e horizonte de expectativas**, concebido com o intuito de realizar um resgate histórico-conceitual acerca dos modelos de responsabilidade civil de intermediários tecnológicos, adotados em países do Norte e do Sul Global.

Este relatório segue o mesmo escopo adotado naquele que o antecede, partindo de análises sobre a legislação vigente nos países estudados e, a partir das discussões de revisão de paradigma jurídico atual e de estruturas dogmáticas da responsabilidade civil, explora os modelos e cenários possíveis de responsabilização de plataformas.

Com base na metodologia da história dos conceitos, a partir, especificamente, do trabalho de Reinhart Koselleck, a presente pesquisa, cujo levantamento primeiro ocorreu ainda em 2020, toma como marcadores básicos a dicotomia do "passado de experiência" (legislações existentes e dogmática jurídica) e "horizonte de expectativas" (modelos possíveis e projetos de lei em andamento).

Embora não se possa reduzir nenhum movimento histórico a pares binários antagônicos, essas antíteses são úteis para analisar intenções, fatos e relações de diversos grupos, a partir das estruturas semânticas neles empregadas e contidas. São, portanto, categorias meta-históricas que servem para analisar contextos diversos (KOSELLECK, 2006, p. 194).

A partir da metalinguagem criada, é possível rastrear os movimentos políticos e técnicos a partir dos conceitos trabalhados e de sua relação com os contextos nos quais estão inseridos. Pela história dos conceitos, portanto, é possível compreender como um círculo social entende uma ideia e a referência a essa ideia, no próprio processo de exaurimento da semiótica que constrói a realidade.

Isso quer dizer que, primeiro, o levantamento bibliográfico busca exaurir um corte temporal vintenário das fontes primárias (leis, discussões políticas e proposições legislativas e governamentais senso largo). Os vinte anos recortam o tempo mínimo, conforme a teoria tradicional da história, de uma geração - por isso, é chamado de recorte gerativo. Não se exclui, dentro das análises, a chamada "aceleração da história" que implica no achatamento dos extratos do tempo. A vintena contada é um marcador base para controle de continuidades e originalidades.

Segundo, a partir do levantamento do passado, é possível construir indicativos sobre as experiências sedimentadas e entender se (e como) o contexto social analisado divide os extratos de tempo histórico (curto, médio, longo). O que é que se mantém, especificamente, como experiência e atravessa o recorte gerativo, chegando a superá-lo?

Um exemplo crítico, no presente ano, é o debate sobre a seção 230, do Communications Decency Act que, ultrapassando um recorte gerativo, mantém influência conceitual até o presente sobre as noções de responsabilidade de intermediário e porto seguro.

Analisar a experiência sedimentada é entender como os sentidos conceituais se localizam no "ponto do tempo" (sincronia) e como ele se modifica no processo sócio-histórico de vivência ao longo do tempo (diacronia). É a diacronia que estabelece as bases da originalidade, enquanto que a sincronia dá os caminhos à cristalização e continuidade de um sentido conceitual.

Pelo mapeamento da relação das dimensões sincrônica e diacrônica é possível entender o horizonte de expectativas de um determinado conhecimento. Se, apelado à semiótica, a relação entre signos determina a sintática, a relação entre signos e usuários, determina a semântica - ambas capturadas no levantamento do passado - então a originalidade e modificação está na relação de signos-usuários-usos, que se conforma na pragmática.

Por isso, essa pesquisa, tomando como base esse marco teórico, é capaz de apontar os sentidos e seus nomes/conceitos antes, durante e depois de determinados processos históricos relevantes - a vantagem de uma metalinguagem é poder falar sobre a linguagem em si, sobre os eventos.

Diante disso, o pressuposto inicial desta pesquisa é o de que a "intermediariedade" tão falada hoje é algo de basilar aos produtos tecnológicos, por instaurarem, em boa parte, algum nível de relação de mediação não estrutural, mas relevante, com o mundo. Uma mediação estrutural, a título comparativo, seria a da linguagem - que permite a forma de conhecer e existir no mundo.

Entretanto, tecnologias de informação e comunicação criam instâncias de experimentação do mundo não constitutivas, portanto não estruturais, mas que modificam comportamentos e a própria linguagem de forma mediata.

Isso vai explicar, ao longo deste levantamento, como o gênero de "provedores de serviços" (todos intermediários, nomeados expressamente ou não) se transforma em, ao menos, três espécies:

a) serviços de provimento de tamanho relevante, com foco na quantidade de usuários como uma medida do poder comercial desses atores;

b) aqueles que, por sua dimensão socioeconômica não podem ser considerados mais meros "provedores", saindo-se de uma dimensão quantitativa, mas uma dimensão qualitativa de capacidade de modificar o cenário político dos países e global (é o debate sobre os gatekeepers) e,

c) plataformas, como uma forma típica de modelos de negócio que é replicada acriticamente dentro da economia de dados.

Aqui também temos um detalhamento do motivo pelo qual as obrigações de intermediários, seu estatuto regulatório e modelos de responsabilização, não se resumem a meramente definir "se há responsabilidade por conteúdo de terceiro" e se essa responsabilidade é "objetiva/subjetiva", "contratual/extracontratual".

Tal ocorre na discussão do art. 19, do Marco Civil da Internet brasileiro, sua constitucionalidade e aplicabilidade. A discussão é relevantíssima, mas ela não exaure toda uma dimensão que vai dos usos e práticas, os sentidos extraídos desses usos e a

criação de modelos para controlar o horizonte de expectativas, especialmente a partir do expediente normativo/legislativo senso estrito. Em um recorte específico, portanto, é possível perceber que a discussão aparece como cortina de fumaça para um debate científico, histórico e técnico-jurídico de maior profundidade.

A escolha metodológica pela classificação dos países conforme os critérios de Norte e Sul Global foi motivada pela facilidade comparativa dos modelos, tendo por referência o projeto político-econômico e social adotado em cada localidade.

Essa forma de classificação surgiu em um contexto multipolar globalizado, a partir da ascensão do capitalismo como sistema socioeconômico dominante e a queda do comunismo, com a dissolução da antiga União Soviética. Em 1980, o termo se popularizou a partir da publicação do relatório da Comissão Brandt, encomendado pelo Banco Mundial, o qual demonstrou a necessidade de aumentar os investimentos nos países do Sul Global e da criação de políticas de cooperação Sul-Sul para lidar com as crises advindas do modelo neoliberal.

Além disso, essas categorias podem ser enquadradas, na teoria de Koselleck, no dualismo dos conceitos antitéticos/assimétricos, tendo em vista que se estabeleceram a partir da negação recíproca uma da outra. Conforme observou Eduardo Galeano, "a história do subdesenvolvimento da América Latina integra, como já foi dito, a história do desenvolvimento do capitalismo mundial". E acrescenta: "O desenvolvimento desenvolve a desigualdade" (GALEANO, 2020, p.8), salientado as contradições que dividem o mundo entre os países que são desenvolvidos e aqueles que não são, devido a um processo (contínuo) de espoliação das suas riquezas.

Assim, além do estigma do subdesenvolvimento, esses conceitos delimitam, no sistema internacional, a identidade de uma geopolítica dominante (Norte), ao lado de outra subalterna (Sul). Contudo, como bem salienta Lucas Ribeiro de Belmont Fonseca:

> [...] em comparação com termos anteriormente utilizados para designar esse agrupamento de países, "Sul Global" carrega consigo um peso político de empoderamento, o que tem se demonstrado adequado, ante a emergência de atores do Sul na condução do sistema internacional [...] (FONSECA, 2016, p. 16).

Isto faz sentido a partir do movimento de resgate das chamadas "Epistemologias do Sul", proposto por autores como Boaventura de Sousa Santos, os quais salientam a importância do desenvolvimento de uma nova forma de compreender o mundo que leve em consideração outros saberes para além do conhecimento tradicional imposto pela ciência moderna ocidental.

Apesar de não haver consenso entre os autores, o Sul Global pode ser definido como "um projeto político permanentemente em disputa por forças progressistas e regressivas da sociedade internacional multipolar" (BALLESTRIN, 2020). Conforme explica Bruno Ayllón Pino (2014), citado por Fonseca, a expressão surgiu no final da

Guerra Fria para:

> [...] fazer referência aos países e às sociedades em desenvolvimento do hemisfério Sul, bem como a outros localizados no hemisfério Norte, que possuem indicadores de desenvolvimento médios e baixos. Estes países são na maioria jovens nações africanas e asiáticas, mas também Estados latino-americanos independentes há mais de dois séculos (PINO, 2014, p. 57 apud FONSECA, 2016, p. 16).

Em termos gerais, o Sul Global abrange países de industrialização tardia, marcados por profundas desigualdades econômicas e sociais e atravessados por um processo de colonizador predatório, além de apresentar processos de rupturas democráticas. A Indonésia representa essa categoria, e a Rússia, em que pese a sua localização geográfica acima da Linha do Equador, também[1].

Nesse estudo, a pesquisa foi desenvolvida com anteparo na perspectiva multissetorial e partindo do contexto sociopolítico e legislativo de quatro países, com levantamentos realizados entre maio de 2022 e janeiro de 2023: **Canadá e Austrália (Norte Global), Rússia e Indonésia (Sul Global)**. A escolha dos quatro países se deu a partir da notícia de implementação de projetos de mudança dos marcos legais de responsabilização de intermediários e, mais, no recorte cultural entre Norte e Sul Global, a partir das convergências e divergências que esses agrupamentos parecem apresentar, em termos de uma identidade de desenvolvimento nacional.

O **método** utilizado é a pesquisa exploratória, elaborada por meio de análise documental (legislações, relatórios, decisões judiciais, jurisprudências) e revisão de literatura.

Os repositórios usados para as pesquisas foram:

a) Stanford University / Wilmap: compilação de vários modelos de responsabilidade civil de intermediários, contendo leis, artigos, comentários, jurisprudências, políticas públicas, relativos a diversos países;

b) School of law / Washington University / Center for Advanced Study and Research on Innovation Policy: com o projeto de pesquisa "The Online Intermediary Liability Research Project"[2];

c) Electronic Frontier Foundation / Platform Liability Trends Around the Globe: Recent Noteworthy Developments[3];

d) Global Network Initiative[4];

e) Australasian Legal Information Institute/ A joint facility of UTS and UNSW Faculties of Law[5];

Outras referências bibliográficas foram obtidas através de pesquisas no Google Scholar ou Google Acadêmico, bem como em redes sociais, como Twitter, considerada importante fonte de manifestação da sociedade civil. Matérias jornalísticas também

1 Segundo Caixeta (2014), a Federação Russa é um país que se enquadra no Sul Global.

2 https://www.law.uw.edu/academics/programs/casrip/liability-research

3 https://www.eff.org/pt-br/deeplinks/2022/05/platform-liability-trends-around-globe-recent-noteworthy-developments

4 https://globalnetworkinitiative.org/policy-issues/intermediary-liability-content-regulation/

5 http://classic.austlii.edu.au/

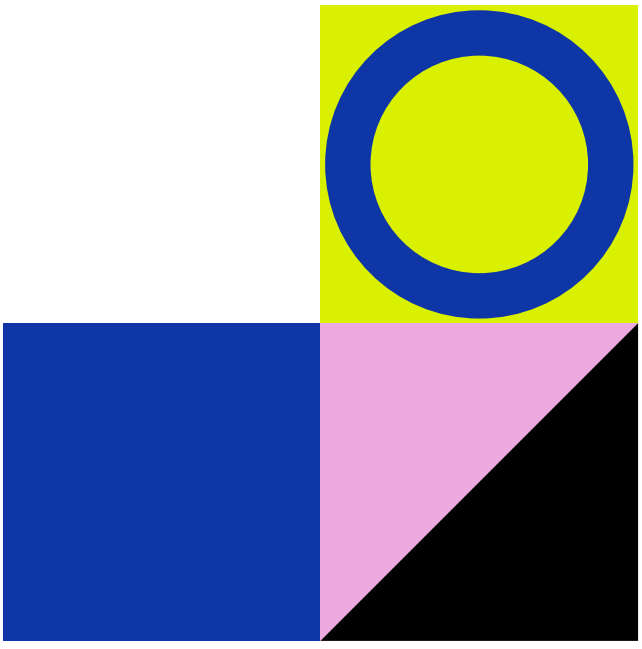
subsidiam a pesquisa, principalmente quando o idioma do país difere dos eleitos paraesta pesquisa.

Dentre os critérios utilizados para a escolha das referências bibliográficas estão a gratuidade do acesso e a escrita em português, inglês ou espanhol. No caso da Rússia, a análise de relatórios, decisões judiciais e leis foi um grande desafio, pois, em sua grande maioria, encontravam-se no original, em cirílico, alfabeto usado para a grafia de línguas eslavas. A tradução desses documentos, na ausência do texto oficial em inglês, foi realizada com o auxílio de ferramentas de tradução automática, como o *Google Translator, Microsoft Translator, DeepL Tradutor e Babylon Translator,* sendo o conteúdo validado e ratificado por artigos e opiniões, escritos nos idiomas escolhidos como critério de pesquisa.

Ademais, o levantamento dos documentos foi organizado, sempre que possível, segundo o enfoque de 04 (quatro) setores da sociedade: governo, sociedade civil organizada, academia e setor privado.

Do setor acadêmico, incluindo a comunidade técnica, foram consultados, majoritariamente, artigos científicos. Da sociedade civil, os documentos levantados variaram entre *policy papers*, artigos de opinião, estudos e recomendações. No setor privado, a pesquisa se debruçou em notícias, artigos de opinião e relatórios de transparência. Por último, do setor governamental, foram examinados , projetos de lei, legislações, decisões judiciais e relatórios de debates públicos.

Feitas as considerações iniciais, a próxima seção traz o resultado do levantamento realizado sobre os modelos de responsabilidade civil de intermediários vigentes nos seguintes países: Austrália e Canadá (Norte Global) e Indonésia e Rússia (Sul Global). Em seguida, são apresentados comparativos conceituais entre as principais terminologias técnico-jurídicas identificadas ao longo da pesquisa, e os comparativos entre os modelos. Ao final, as principais conclusões obtidas como resultado das investigações são expostas.



O NORTE GLOBAL

1 AUSTRÁLIA

1.1 Considerações iniciais

Localizada na Oceania, a Austrália é um país democrático que faz parte da chamada Comunidade Britânica de Nações *(Commonwealth)*. O rei da Inglaterra (Charles III) é o Chefe de Estado australiano, sendo, no entanto, representado no país pelo Governador-Geral. Trata-se, nesse sentido, de uma monarquia constitucional que adota o parlamentarismo como sistema de governo. O poder é exercido, de fato, pelo Primeiro-Ministro, que é escolhido por meio de eleições gerais a partir da indicação do partido ou coalizão com maior representação na Câmara.

No que tange ao cenário da Governança da Internet, a Austrália possui uma ampla infraestrutura de Tecnologias de Informação e Comunicação (TIC), com rede de computadores acessível e disponível para grande parte da população (FREEDOM HOUSE, 2022). Estima-se que mais de 91% australianos estavam conectados à Internet, em 2022 (HUGHES, 2022). No entanto, diante do aumento das preocupações do Governo com o terrorismo, o *cyberbulling*, divulgação de imagem íntima, abuso infantil e discurso de ódio na rede, a regulação dos provedores de serviços da Internet (ISP), em especial das plataformas de mídias sociais e mensageria, ainda continua em discussão no país.

Atualmente, a responsabilidade civil de intermediários tecnológicos é regulada por leis que não estão sistematizadas em um único corpo de normas, de modo que várias doutrinas foram se desenvolvendo de forma diversa ao longo do tempo, tornando os requisitos de incidência das normas confusos e até mesmo incoerentes em torno da questão (PAPPALARDO; SUZOR, 2020, p. 282).

Em geral, pode-se dizer que o sistema de responsabilização australiano é baseado no "conhecimento real" do intermediário (OMOND et al, 2021, p. 8) e, consequentemente, na sua capacidade de remover, após a sua ciência, os conteúdos previstos na lei ou que violem o direito de terceiros. A responsabilidade depende, portanto, do grau de ciência dos provedores sobre os conteúdos ilícitos disponibilizados em seus serviços (ou da "probabilidade razoável" do conhecimento da sua presença), seja porque eles "autorizaram" a prática danosa (não adotando, quando podiam, as medidas técnicas cabíveis para evitar o dano), seja porque tenham, de alguma forma, "incentivado" a prática de atos ilícitos. Além dessas hipóteses, os provedores que exerceram algum tipo de controle editorial, mesmo que mínimo, também podem ser responsabilizados, especialmente nos casos de difamação e propaganda enganosa.

Em 2022, entrou em vigor o *Online Safety Act*, lei que ampliou ainda mais os deveres dos intermediários, bem como os poderes do *eSafety Commissioner*, agência governamental que, ao lado da *Australian Communications and Media Authority* (ACMA), é responsável por gerir e fiscalizar a segurança da Internet no país. Com as alterações

promovidas pela lei, ainda é possível que provedores sejam responsabilizados se, após notificação do *eSafety Commissioner Office*, falharem em remover, dentro de 24 horas, os conteúdos definidos como "prejudiciais".

Além dessa lei, outros projetos foram aprovados nos últimos anos e podem colocar em risco os direitos fundamentais e liberdades individuais, favorecendo a censura e a ocorrência de práticas vigilantistas na Austrália.

1.2 Autoridades Administrativas

1.2.1 Autoridade Australiana de Comunicação e Mídia

A *Australian Communications and Media Authority* (ACMA) é uma autoridade estatal independente responsável por regulamentar os serviços de radiodifusão, Internet, radiocomunicações e telecomunicações no país. As suas funções estão previstas em leis como o Broadcasting Services Act 1992, *Telecommunications Act* 1997, e *Australian Communications and Media Authority Act 2005* (AUSTRÁLIA, [20--]).

Em linhas gerais, a ACMA atua:

a) no monitoramento do setor de comunicações, incluindo tratamento de reclamações, manutenção de registros, emissão de pareceres e realização de inspeções, investigações e inquéritos;

b) na fiscalização da aplicação dos códigos e padrões do setor, impondo sanções, penalidades civis e advertências quando necessário;

c) na emissão de licenças e na manutenção de padrões aplicáveis e na criação de padrões de licenciamento e códigos de registro aplicáveis;

d) na cobrança de taxas e impostos e na alocação de recursos;

e)no gerenciamento de padrões internacionais e no fornecimento de informações aos consumidores; e

f) na condução de programas educacionais, na produção de pesquisas e relatórios para o Governo (AUSTRÁLIA, [20--]).

Além disso, a ACMA é responsável por aprovar os padrões e códigos de prática criados pelas indústrias do setor. Isso porque a Austrália possui um esquema de co-regulação de conteúdo. Dessa forma, o *Communications Alliance*[6], principal organização que representa a indústria de comunicações do país, pode propor padrões para o setor e os submeter à aprovação da Autoridade Administrativa. Assim, além da legislação aplicável, os intermediários acabam sendo regulados, de forma conjunta, pelas resoluções expedidas pelo ACMA e pelos códigos produzidos pelo setor.

Com a aprovação do *Online Safety Act*, o Governo anseia que os provedores desenvolvam códigos de práticas e padrões para o setor com o objetivo de coibir o

6 *Communications Alliance* é uma organização que representa as indústrias de telecomunicações australianas, com o objetivo de oferecer contribuições e desenvolver códigos de práticas e padrões para o setor.

compartilhamento de materiais considerados prejudiciais, atendendo para as chamadas *Basic Expectations of Online Safety* (BESO), que compreende um conjunto de orientações que devem ser seguidas pelos provedores serviços online.

1.2.2 eSafety Commissioner

Em 2015, o *Enhancing Online Safety Act* instituiu o *eSafety Commissioner* para atuar junto com a *Australian Communications and Media Authority* (ACMA), na promoção de segurança para crianças e adolescentes, na Internet. Assim como a ACMA, o *eSafety Commissioner* é uma agência independente do Governo australiano.

Dois anos depois do *Enhancing Online Safety Act* entrar em vigor, o governo decidiu ampliar o escopo da lei para que o órgão fosse responsável por proteger não apenas crianças e adolescentes, mas também cidadãos adultos. Assim, o *Office of the Children's eSafety Commissioner* passou a se chamar *Office of the eSafety Commissioner* (ou simplesmente, *eSafety Commissioner*) e abarcar novos grupos sociais, administrando também questões que envolvam violência doméstica, divulgação não consensual de imagens íntimas e segurança de idosos na Internet.

A função principal do comissário é administrar as reclamações e objeções feitas em seu portal e aplicar, quando cabível, sanções civis e administrativas. Atualmente, esse cargo é chefiado por uma mulher, Julie Inman Grant. Além da Comissária, educadores, investigadores, advogados, analistas de políticas, especialistas em tecnologia, especialistas digitais fazem parte da equipe que atua na agência (AUSTRÁLIA, [202-]b).

Em 2022, o *Online Safety Act 2021* entrou em vigor e aumentou a capacidade de atuação do *eSafety Commissioner* que, além de gerir os esquemas de denúncia, passou a fiscalizar a conformidade dos provedores de serviços online com as *Basic Expectations of Online Safety* (BESO), bem como coordenar atividades com outros órgãos para a manutenção da segurança online dos cidadãos australianos e estabelecer padrões e regras caso os códigos de práticas que forem desenvolvidos de forma voluntária pela indústria não satisfaçam as exigências da lei (AUSTRÁLIA, [202-]a).

O *eSafety Commissioner* também poderá ordenar, em situações de crise, o bloqueio ao acesso a sites que hospedem "material violento abominável" por um período de até três meses, podendo ser renovado por tempo indeterminado, a critério da agência. Além disso, poderá requerer, diretamente, dados que permitam a identificação do usuário suspeito, antes concedidos apenas mediante ordem judicial, e compartilhá-los com outros órgãos.

1.3 O arcabouço legal

1.3.1. *Copyright Act 1968* (Cth)

Sob a égide da chamada *authorisation liability*, infringe a lei de direitos autorais quem, não sendo o proprietário e sem a permissão deste, utiliza obra literária, teatral, musical ou artística ou autoriza alguém a cometer violações (AUSTRÁLIA, 1968).

Com base nas seções 36 (1) e 101 (1) do *Copyright Act* 1968, os reclamantes podem argumentar que o provedor de serviço não atuou como mero facilitador de um determinado serviço (39 B e 112 E), mas contribuiu de forma ativa, "autorizando" práticas ilegais, uma vez que poderia ter atuado, quando notificado, ou tomado as precauções necessárias para evitar que o dano ocorresse (AUSTRÁLIA, 1968).

Os intermediários são normalmente responsabilizados em torno do conceito de *"authorise"*. Para isso, tenta-se demonstrar que ele, de alguma forma, sancionou, aprovou ou permitiu que os usuários praticassem violações por meio de ferramentas e/ou sistema que disponibiliza e que, quando notificado, não tornou indisponível o conteúdo violador.

De acordo com Pappalardo (2015, p.3), recentemente a Suprema Corte da Austrália criticou o fato de que o conceito de *"authorise"* ter sido definido a partir de palavras como *"sanction", "approve"* e *"countenance"*, termos que não têm "significado legal fixo dentro da lei de direitos autorais". Além disso, palavras como *"countenance"* possuem outros significados que não são coextensivos com o entendimento comum que se tem do termo *"authorise"* .

A lei estabelece portos seguros *(safe harbours)* para os *"Carriage Service Providers"* (CSP), definidos pelo *Telecommunications Act 1997* como espécie de ISP prestadores de serviço de transporte. A Subdivisão B do *Copyright Act 1968*, por sua vez, prevê quatro categorias de atividades desempenhadas que são consideradas relevantes para os fins da lei, apresentadas na tabela 1.

Categorias	Categoria A: Transmissão	Categoria B: Cache	Categoria C: Hospedagem	Categoria D: Pesquisa
Definição	Fornece instalações ou serviços para transmissão, roteamento ou fornecimento de conexões para materiais protegidos por direitos autorais, ou o armazenamento intermediário e transitório durante a transmissão, roteamento ou fornecimento de conexões.	Armazena em cache material por meio de um processo automático. O *"Carriage Service Provider"* não deve selecionar manualmente o material protegido por direitos autorais para armazenamento em cache.	Armazena, sob a direção de um usuário, material protegido por direitos autorais em um sistema ou rede controlado ou operado pelo ou através *"Carriage Service Provider".*	Encaminha os usuários para um local online usando ferramentas ou tecnologia de localização de informações.

Tabela 1: Categorias de atividades dos provedores de Internet, segundo Subdivisão B do *Copyright Act 1968*

Cada uma das categorias deve observar as condições previstas na tabela 2.

Categorias	Categoria A: Transmissão	Categoria B: Cache	Categoria C: Hospedagem	Categoria D: Pesquisa
Definição	1. Qualquer transmissão de material protegido por direitos autorais na realização desta atividade deve ser iniciada por/ou sob a direção de uma pessoa que não seja o Carriage Service Provider. 2. O Carriage Service Provider não deve fazer modificações substanciais no material de direitos autorais transmitido. Isso não se aplica a modificações feitas como parte de um processo técnico.	1. Se o material protegido por direitos autorais armazenado em cache estiver sujeito a condições de acesso do usuário no site de origem, o *Carriage Service Provider* deve garantir que o acesso a uma parte significativa do material seja permitido apenas aos usuários que atenderem a essas condições. 2. Se houver um código relevante do setor em vigor - o *Carriage Service Provider* deve cumprir as disposições relevantes do código relacionadas a: (a) atualização do material protegido por direitos autorais armazenado em cache; e (b) não interferência na tecnologia usada no site de origem para obter informações sobre o uso do material protegido por direitos autorais. 3. O *Carriage Service Provider* deve remover ou desabilitar rapidamente o acesso ao material protegido por direitos autorais em cache mediante notificação do proprietário na forma prescrita na lei. 4. O *Carriage Service Provider* não deve fazer modificações substanciais no material armazenado em cache à medida que é transmitido a usuários subsequentes. Isso não se aplica a modificações feitas como parte de um processo técnico.	*1.* O "Carriage Service Provider" não deve receber um benefício financeiro diretamente atribuível à atividade infratora desde que tenha a capacidade de controlar a atividade. *2.* O Carriage Service Provider deve remover ou desabilitar rapidamente o acesso ao material que reside em seu sistema ou rede após o recebimento de um aviso de que o material foi considerado ilícito por um tribunal na forma prescrita pela lei. 2A. O Carriage Service Provider deve agir rapi-damente para remover ou desabilitar o acesso ao material protegido por direitos autorais que armazenado em seu sistema ou rede se: (a) to-mar conhecimento de que o material infringiu a lei de direitos autorais; ou (b) tomar conheci-mento de fatos ou circunstâncias que tornem aparente que o material provavelmente está infringindo a lei de direitos autorais. 3. O Carriage Service Provider deve cumprir o procedimento prescrito em relação à remoção ou desabilitação do acesso ao material prote-gido por direitos autorais que reside em seu sistema ou rede.	

Tabela 2: Condições a serem cumpridas, por categorias de atividades dos provedores de Internet.

A imunidade para esses provedores é limitada, vez que devem atender a eventuais ordens cautelares expedidas pelos tribunais[7]. Se o provedor deixar de remover o conteúdo ou bloquear uma conta infringente, por exemplo, será responsabilizado.

Para todas as categorias, é obrigatória a previsão, nos termos da política de uso do aplicativo, do encerramento da conta de usuários infratores reincidentes, em "circunstâncias apropriadas"[8].

Nos anos 2000, o *Copyright Amendment* (Agenda Digital) inseriu uma nova subseção na lei, com o objetivo de trazer maior segurança jurídica para os provedores. Segundo Seção 36 ss (1A), se uma pessoa autorizar, sem a licença do proprietário, praticar qualquer ato compreendido como direitos deste, violará a lei de direitos autorais do país. Deve-se ponderar também:

a) a extensão (se houver) do poder da pessoa para impedir a prática do ato em questão;

b) a natureza de qualquer relação existente entre a pessoa proprietária dos direitos autorais e a pessoa que praticou o ato em questão;

c) se a pessoa tomou quaisquer medidas razoáveis para prevenir ou evitar a prática do ato, incluindo se a pessoa cumpriu quaisquer códigos de conduta relevantes da indústria (AUSTRÁLIA, 2000).

A Seção 39 B e 112 E do *Copyright Amendment* (Agenda Digital) 2000 estabelece quando a disponibilização de uma determinada funcionalidade se transforma em uma verdadeira "autorização" para transgredir a lei, que difere quando atua como um "mero canal", fornecendo apenas os meios técnicos pelos quais a violação de direitos autorais ocorre.

Com o Acordo de Livre Comércio Austrália-Estados Unidos (AUSFTA), em 2004, foram introduzidas mudanças na legislação australiana para adequar as normas de direitos autorais ao *Digital Millennium Copyright Act* (DMCA), a partir da adoção de medidas como: o aumento do prazo para as obras caírem em domínio público, a ampliação do uso de restrições tecnológicas para utilização de obras digitais, a adoção de *"safe harbors"* e o estabelecimento do regime de *"notice and takedown"* (AUSTRÁLIA, 2004).

Diante desse acordo, a Austrália adotou controles mais rígidos e amplos de proteção aos direitos autorais, o que beneficiou especialmente empresas do setor de entretenimento, em prejuízo dos cidadãos australianos (RIMMER, 2006). Além disso, aumentaram os riscos para outros intermediários, como bibliotecas, instituições culturais, operadoras de telecomunicações e ISPs, conforme salienta Matthew Rimmer (2006).

Na Austrália, há três procedimentos de notificação para a remoção de conteúdos que violem a lei de direitos autorais *(takedown notice)*[9]. O primeiro *(owner notice)* é para

---

7 De acordo com a Seção 115A(1) do Copyright Act (AUSTRÁLIA, 1968), o proprietário dos direitos autorais pode solicitar ao Tribunal Federal Australiano medida liminar quando: a) o ISP fornece acesso a um local online fora da Austrália, b) a localização ajuda a infringir ou facilita a violação de direitos autorais, e c) o principal objetivo da localização é infringir ou facilitar a violação de direitos autorais, seja na Austrália ou não. Dessa forma, o tribunal pode determinar que o ISP bloqueie o acesso a um site ou aplicativo, encerre uma conta específica, indisponibilize o material infrator ou qualquer outra ordem não monetária menos onerosa equivalente.

8 Subdivisão D do *Copyright Act 1968* (AUSTRÁLIA, 1968).

9 Na Austrália, adota-se a expressão "takedown notice" para se referir ao aviso de remoção de conteúdo, previsto no

situações em que o proprietário ou quem o represente tenha motivos razoáveis para acreditar que o conteúdo hospedado pelo provedor infringe seus direitos. O segundo *(SP initiated takedown)*, por sua vez, é indicado para os casos em que o próprio provedor de serviços percebe que o material hospedado por ele viola direitos de terceiros. Por fim, o terceiro *(link notice)* é para os casos em que o proprietário percebe que o provedor está indexando links ou referências a um material considerado violador, o que ocorre especialmente com mecanismos de busca (KIMBERLEY EVANS, ALLENS PATENT & TRADE MARK ATTORNEYS, 2021, p. 11).

Apesar dos procedimentos possuírem algumas diferenças, em geral, após o aviso de retirada, se o provedor remover e bloquear, rapidamente, o acesso ao conteúdo indicado, não será responsabilizado pela conduta do usuário. Caso o provedor não colabore, o proprietário deverá obter uma ordem judicial para que o conteúdo seja removido, sendo possível a responsabilização subsidiária desse provedor. Na Divisão 2AA do *Copyright Act*, estão disponíveis recursos para que os reclamantes acionem a Justiça contra os provedores em caso de violação. O Anexo 2 do *Copyright (International Protection) Regulations* (1969) também fornece vários tipos de formulários que podem ser utilizados para notificar provedores de serviços (KIMBERLEY EVANS, ALLENS PATENT & TRADE MARK ATTORNEYS, 2021, p. 8-9).

Por fim, a Seção 115A introduzida pelo *Copyright Amendment (Online Infringement) Act* de 2015 permite que os juízes concedam liminares que desabilitem o acesso a serviços online hospedados fora da Austrália. Para isso, o proprietário deve demonstrar que o site estrangeiro infringiu diretamente a lei ou "facilitou" a sua violação. No entanto, para determinar o bloqueio de um site, o Tribunal deverá analisar uma série de fatores, que incluem a verificação da proporcionalidade da medida, o impacto dela para as pessoas não relacionadas com a violação e o interesse público envolvido (AUSTRÁLIA, 2015a). Em 2018, o *Copyright Amendment (Online Infringement) Act* de 2018 estendeu essas regras para os *carriage service providers* e para os *online search engine providers.*

1.3.2 *Racial Discrimination Act* 1975 (Cth)

De acordo com a Seção 18 C do *Racial Discrimination Act* 1975, é ilegal ofender, insultar, humilhar e intimidar uma pessoa ou um grupo de pessoas por questões de raça, cor ou origem nacional ou étnica (AUSTRÁLIA, 1975b). Nesses casos, será avaliada a probabilidade do ato - que deve ser público - causar danos. Assim, com fundamento nessa lei, provedores que, por exemplo, disponibilizam fóruns onlines na Internet podem ser responsabilizados por "facilitar" os meios para os quais os usuários postem comentários ofensivos ou falhem em remover conteúdos de natureza discriminatória. O problema, nesses casos, é identificar quando essas falhas são motivadas por razões discriminatórias do próprio provedor.

Anexo 10 do *Copyright Regulations 1969.*

1.3.3 *Broadcasting Services Act* 1992 (Cth)

O *Broadcasting Services Act* (BSA) traz uma limitação geral de responsabilização para os *"Internet Service Provider"* (ISP) e os *"Internet Content Host"* (ICH), incluído pelo *Broadcasting Services Amendment (Online Services) Act* (OSA), em 1999. De acordo com o Cl 91 (1) *schedule* 5, não têm efeito leis de um Estado ou território australiano que responsabilizem (civil ou criminalmente) um provedor por transportar ou hospedar conteúdos ilícitos dos quais ele não tenha ciência, nem exigir que ele monitore o conteúdo ou mantenha registros do material que circula em seu site (AUSTRÁLIA, 1992).

No entanto, tanto o ISPs quanto os ICHs ainda devem cumprir as regras definidas para a categoria dos *Online Content Service Providers*, que estabelecem que, ao tomar conhecimento do material ilícito, os provedores devem adotar as medidas cabíveis. Nos termos da lei, considera-se *Online Content Service Provider* todo provedor que fornece conteúdo online através de seu site ou por outro intermediário de Internet, incluindo plataformas que controlam, geram ou filtram conteúdo.

É importante ressaltar que a imunidade que a cláusula fornece, em relação à manutenção de registros, diz respeito apenas aos provedores que fornecem "conteúdos de Internet", os quais compreendem informações que (AUSTRÁLIA, 1992):

a) são mantidas em um dispositivo de armazenamento de dados; e

b) são cedidas, ou estão disponíveis para acesso, através de um serviço de transporte da Internet;

No entanto, não incluem: correio eletrônico comum; ou informações que são transmitidas na forma de um serviço de radiodifusão (Cl 3 of Sch 5). Isso acaba expondo os ICHs a potenciais riscos, uma vez que muitos serviços de *streaming* podem se enquadrar na definição de um serviço de radiodifusão. Além disso, uma diretiva aprovada pelo governo determinou que um serviço que disponibiliza programas de televisão ou programas de rádio através da Internet não deverá ser considerado um serviço de radiodifusão, para efeitos da lei, o que torna ainda mais complexa a definição (KHEIR; ALAMEDDINE; AFIOUNY, 2020, p.5).

Conforme alerta o relatório do Wilmap CIS - Stanford, a cláusula 91(1):

> *provides little additional protection from the common law tort of defamation, as amended by legislation of Australian States and Territories, which applies to anyone who 'publishes' a defamatory imputation. While there are defences for 'innocent dissemination' which will apply to internet intermediaries who are publishers, these defences evaporate once the intermediary is put on notice, at which point Cl 91(1) will no longer apply* (THE CENTER FOR INTERNET AND SOCIETY, [s.d])[10].

Além disso, a lei permite ainda que a ACMA edite regras, por meio de instrumento legislativo, sobre esses provedores, além de dar autonomia ao órgão para que tome decisões de natureza administrativa.

10 Tradução livre: "oferece pouca proteção adicional contra o delito de difamação da lei comum, conforme alterado pela legislação dos estados e territórios australianos, que se aplica a qualquer pessoa que 'publique' uma imputação difamatória. Embora existam defesas para 'disseminação inocente' que se aplicarão a intermediários da Internet que são editores, essas defesas desaparecem quando o intermediário é notificado, momento em que o Cl 91(1) não será mais aplicável".

1.3.4 Telecommunications Act 1997 (Cth)

A Seção 87 do Telecommunications Act 1997 traz a definição de Carriage Service Providers (CSP) como aqueles que fornecem serviços de telecomunicações através de:

a) unidades de rede que uma operadora licenciada possui; ou

b) unidades de rede cobertas por uma Declaração de Transportadora Nomeada (NCD), concedida pelo ACMA (AUSTRÁLIA, 2022a).

Além disso, a Seção 313 (3), Volume 2 do Telecommunications Act 1997 possibilita que as autoridades solicitem informações de Internet Service Providers (ISPs) para auxiliar no:

a) cumprimento da lei penal e das leis que impõem penalidades pecuniárias;

b) na aplicação das leis penais em vigor em um país estrangeiro;

c) na investigação e no julgamento de crimes da jurisdição do Tribunal Penal Internacional (na acepção do International Criminal Court Act 2002) e ofensas judiciais (na acepção do International War Crimes Tribunals Act 1995);

d) proteção da Receita Pública; e

e) salvaguardar a segurança nacional (AUSTRALASIAN LEGAL INFORMATION INSTITUTE, 1997).

Dessa forma, a lei é utilizada como fundamento jurídico para permitir que agências do Governo possam bloquear websites mediante requerimento ao ACMA, de modo que é dispensável o detalhamento da solicitação caso:

a) esteja fundamentada na aplicação da lei vigente;

b) seja relativa à segurança nacional, ou

c) possa prejudicar o andamento das investigações ou atividades operacionais (AUSTRALASIAN LEGAL INFORMATION INSTITUTE, 1997).

1.3.5 *Spam Act* 2003 (Cth)

A subseção (1) da Seção 16 do *Spam Act* 2003 torna ilegal o envio de mensagens comerciais eletrônicas não solicitadas (AUSTRÁLIA, 2003). Para que seja possível o envio de email, é necessário obter a permissão do usuário, que poderá ser tácita ou expressa. Além disso, a norma não se aplica se aquele que enviou a mensagem não sabia ou não poderia, com razoável diligência, ter verificado que a mensagem tinha um link australiano, ou ainda se enviou por engano, possuindo em todos os casos o ônus de provar isso - conforme subseções (3) (4).

É importante notar ainda que até mesmo mensagens comerciais enviadas com o consentimento do destinatário devem identificar o remetente, disponibilizar detalhes do contato e possibilitar mecanismos que facilitem o cancelamento da assinatura (AUSTRÁLIA, 2022b).

1.3.6 *Uniform Defamation Acts* (UDA)

A legislação sobre difamação tem como objetivo principal proteger a reputação dos australianos. Cada estado e território possui uma regulação própria, mas entre 2005 e 2006 foram aprovadas *Uniform Deformation Acts*, que buscaram trazer mais congruência para o tema no país.

De acordo com o *Freedom House* (2022), as leis australianas de difamação estão entre as mais favoráveis aos reclamantes no mundo, o que acaba gerando um efeito de autocensura na mídia e, até mesmo, entre usuários comuns, que por medo de processos judiciais, acabam muitas vezes evitando expressar suas opiniões.

O conceito de difamação abarca tanto ofensas verbais *(slander)* quanto escritas *(libel)*, podendo ser tanto explícito quanto implícito *(innuendo)*. Para que os infratores sejam responsabilizados são analisados: o conteúdo da publicação, o autor, a publicidade e o grau da ofensa. Trata-se, portanto, de responsabilidade objetiva *(strict liability)*, já que é dispensável a verificação da culpa.

Em relação ao conteúdo da difamação, os tribunais australianos realizam um teste para verificar se o conteúdo difamatório tem realmente a capacidade de diminuir a estima do ofendido na comunidade ou levará uma pessoa comum e razoável a pensar menos na outra. Nesses casos, a motivação é irrelevante, apesar de haver defesas que podem ser arguidas na mensuração do dano.

No que tange ao autor da ofensa, este deve ser minimamente identificável, utilizando como parâmetro a capacidade de um "cidadão razoável". Além disso, é avaliada a publicidade da ofensa, ou seja, se ela é pública ou, ao menos, foi comunicada a outra pessoa. Por fim, os juízes verificam se a ofensa causou um dano grave à reputação.

Há algumas defesas que podem ser levantadas pelos réus para se proteger das acusações, como:

a) verdade sobre as palavras proferidas *(contextual truth)*;

b) opinião honesta *(honest opinion)*, apresentada como uma opinião pessoal e não um fato;

c) disseminação inocente *(innocent dissemination)*, quando não se sabia ou quando não é possível saber que se tratava de conteúdo difamatório, sendo a falta de conhecimento um fator determinante para afastar a responsabilização; e

d) publicação de matéria que é de interesse público *(publication of matter concerning issue of public interest)*, cujo conceito fala por si (AUSTRÁLIA, 2012b).

De acordo com o *Report of Regulation of Digital Media and Intermediaries*, a responsabilidade dos provedores de Internet é regulada da mesma forma que os outros meios de comunicação de massa, o que leva à possibilidade de serem responsabilizados pela publicação de um conteúdo difamatório. Nesse sentido, qualquer agente envolvido na cadeia de publicação da ofensa, como operadores de sítios web, fóruns de discussão, mecanismos de busca e quem disponibiliza conteúdo de terceiros, pode ser responsabilizado (OMOND et al, 2021, p. 36).

A limitação da responsabilidade nesses casos encontra-se no *Broadcasting Services Act*, analisado anteriormente, que traz imunidades para os ISPs e ICHs quanto ao conteúdo considerado ofensivo, incluindo material difamatório. Essa imunidade

possui várias deficiências que expõem especialmente os provedores de hospedagem que prestam serviços que não estão compreendidos na definição de *"Internet Content"*. Dentre estes, destacam-se os mecanismos de buscas como o Google.

As imunidades acabam, portanto, dependendo da demonstração por parte do provedor de que não tinha conhecimento sobre o material difamatório, nem interferiu na escolha do material ou realizou qualquer tipo de edição no conteúdo que será divulgado. Nestes últimos casos, faz-se uma analogia com os editores de jornais e emissoras de rádio e TV. Até mesmo provedores com o papel menos ativo, como aqueles que disponibilizam fóruns de discussão, podem ser responsabilizados como "editores secundários" se sabiam, ou teriam como saber, que havia conteúdo difamatório em suas plataformas.

Em 2021, os estados de *New South Wales*, Victoria e South Australia aprovaram novas alterações em suas leis de difamação. De acordo com a organização *Freedom House*, as mudanças que entraram em vigor podem ajudar a diminuir os processos por difamação no futuro, principalmente em relação àqueles iniciados contra usuários de mídia social e jornalistas que publicam informações de interesse público (FREEDOM HOUSE, 2022).

1.3.7 *Enhancing Online Safety for Children Act 2015 (Cth)*

Em 2015, entrou em vigor o *Enhancing Online Safety for Children Act* 2015 com o objetivo de estabelecer salvaguardas para as crianças no ambiente online, coibindo o chamado *"cyberbullying"*. Dessa forma, foi criado o chamado *"Office of the Children's eSafety Commissioner"* para auxiliar o ACMA, mencionado acima, na remoção de conteúdos ofensivos para esse grupo.

De acordo com *Reviews of the Enhancing Online Act* 2015 e *the Online Content Scheme*, cabia ao *eSafety Commissioner*:

a) monitorar a conformidade com os códigos e padrões da indústria de serviços de conteúdo e internet;

b) aconselhar e auxiliar pais e responsáveis em relação à supervisão e controle do acesso de crianças à Internet;

c) conduzir e coordenar programas de educação comunitária com grupos e agências relevantes; realizar e encomendar pesquisas;

d) estabelecer contato com órgãos reguladores e outros órgãos relevantes no exterior; e aconselhar o governo sobre assuntos relacionados ao exercício de suas funções (AUSTRÁLIA, 2018a).

1.3.8 *The Telecommunications and Other Legislation (Access and Assistance) Act 2018*

Em 2019, entrou em vigor o *Access and Assistance Act* 2018, lei que obriga empresas de tecnologia a fornecer, para fins de investigação e segurança nacional, o

acesso a comunicações criptografadas às agências estatais (AUSTRÁLIA 2018a). A lei também determina a instalação de vulnerabilidades para o acesso a informações, pondo em risco a manutenção da criptografia não só na Austrália, mas também no mundo inteiro (RODRIGUES; VIEIRA, 2018).

No *"Statement of Principles on Access to Evidence and Encryption"*, Estados Unidos, Reino Unido, Canadá, Austrália e Nova Zelândia (os chamados *"Five Eyes"*) afirmam que, apesar da criptografia ser essencial para garantir a segurança no ambiente digital e a proteção de informações pessoais, comerciais e governamentais, a privacidade não é um direito absoluto (AUSTRÁLIA, 2018b). Dessa forma, abrem espaço para a possibilidade de enfraquecimento desses sistemas de proteção para acesso a informações, com o objetivo de combater crimes e ameaças à segurança nacional e global.

Em nota à imprensa, a *Apple* afirma que, além de ambíguos e genéricos, os termos da lei australiana estabelecem um poder sem precedentes para o Estado e coloca em risco a segurança de todos os usuários (MENDES, 2018). Segundo a Freedom House (2022):

> Rights groups have criticized the Assistance and Access law's broad reach, relative lack of oversight, and harsh penalties. Opponents have also raised concerns about its potentially stifling effect on the country's technology sector, as local companies could be forced to create products that are less secure than those of their foreign competitors[11].

1.3.9 *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019*

Após o atentado de *Christchurch*, na Nova Zelândia, que teve as cenas do massacre divulgadas ao vivo no perfil do *Facebook* do atirador (GRIFFITHS, 2019), foi aprovado o *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act* 2019, que amplia as hipóteses de responsabilização objetiva *("strict liability")* dos intermediários, criando um regime de *notice and takedown* mais rigoroso do que o que está em vigor nos EUA e na Europa (AUSTRÁLIA, 2019).

De acordo com a lei, os provedores *(Internet Service Providers, Content Service Providers e Hosting Service Providers)* serão responsabilizados criminalmente se falharem em deixar de hospedar ou de remover rapidamente conteúdo definido na lei como "abominável" (Seção 474.34). De acordo com as seções v. 474.31 e v.474.32, conteúdo "abominável" é definido como todo material de áudio, vídeo e audiovisual que registre ou transmita condutas consideradas ofensivas por pessoas razoáveis e que envolvam terrorismo, assasinato (ou a tentativa), tortura, estupro e sequestro (AUSTRÁLIA, 2019).

No entanto, a incidência da norma é afastada nos casos em que a divulgação desses materiais está relacionada à Seção v. 474.37, ou seja, nos casos de:

11 Tradução livre: "Grupos de direitos criticaram o amplo alcance da lei de assistência e acesso, a relativa falta de supervisão e as penalidades severas. Os oponentes também levantaram preocupações sobre seu efeito potencialmente sufocante no setor de tecnologia do país, já que as empresas locais podem ser forçadas a criar produtos menos seguros do que os de seus concorrentes estrangeiros".

a) cumprimento da lei;

b) condução de processos em um tribunal;

c) realização de pesquisa científica, médica, acadêmica ou histórica;

d) reportagem ou relatório, que sejam de interesse público e/ou tenham sido produzido por uma pessoa que trabalha profissionalmente como jornalista;

e) desempenho de funções públicas;

f) alteração de lei ou precedente; e

g) desenvolvimento, execução, exibição ou distribuição de boa fé de uma obra artística (AUSTRÁLIA, 2019).

Há outra exceção para os casos de comunicação política[12], a qual tem respaldo na Constituição Australiana.

Em caso de descumprimento, a lei prevê penas de 3 anos de prisão e multa de até US $2,22 milhões para pessoas físicas e de até US $11,1 milhões ou 10% do faturamento anual da empresa para pessoas jurídicas (AUSTRÁLIA, [entre 2019 e 2022]).

Além da rápida tramitação pelo Congresso da Austrália, a lei é criticada por distribuir todo o ônus da prova aos provedores, que terão ainda que lidar com o conceito indeterminado de *"expeditious"*, rapidamente, em tradução livre (SHIEBER, 2019).

1.3.10 *Treasury Laws Amendment (News Media and Digital Platforms Mandatory Bargaining Code) Act 2021*

Sob a legislação de proteção aos consumidores, os intermediários podem ser responsabilizados por propagandas fraudulentas e enganosas que induzam o consumidor ao erro produzidas por terceiros.

Em 2021, foi aprovado o *Treasury Laws Amendment (News Media and Digital Platforms Mandatory Bargaining Code) Act* que altera o *Competition and Consumer Act* com o objetivo de equilibrar o poder de mercado entre empresas de mídia de notícias australianas e as plataformas digitais, como *Google* e *Facebook*, em relação à disponibilização de conteúdo jornalístico nessas plataformas (AUSTRÁLIA, 2022c).

O *News Media and Digital Platforms Mandatory Bargaining* Code prevê um regime de arbitragem obrigatório para que as empresas negociem com veículos de notícias o pagamento para a inclusão de notícias nas plataformas. A lei, contudo, deixa aberto o conceito de "plataformas digitais" para incluir todo tipo de prestadora de serviço online. De acordo com a seção 52E do Código, cabe ao ministro do *Department of the Treasury* determinar quais empresas estão sujeitas a essa lei (AUSTRÁLIA, 2021i).

Após a aprovação do *News Media and Digital Platforms Mandatory Bargaining Code*, o *Facebook* adotou medidas de retaliação, bloqueando e restringindo conteúdos na Austrália. De acordo com a *Freedom House*, a plataforma só reverteu o bloqueio após o governo australiano concordar em fazer concessões, dando, por exemplo, mais tempo para negociação de acordos com empresas de notícias e estabelecendo um período de aviso prévio (FREEDOM HOUSE, 2022).

12 Na Austrália, a Constituição não protege de forma explícita o direito à liberdade de expressão. No entanto, infere-se que há um direito implícito à liberdade de comunicação política relacionado ao exercício da democracia. Não se trata, nesse sentido, de um direito individual dos cidadãos australianos, mas sim uma limitação ao poder do Estado de interferir na livre comunicação das pessoas.

Ainda segundo a mesma organização:

> Critics have said that the News Media Bargaining Code ensures that major news corporations benefit from the 'systematic data collection and exploitation models' that digital platforms promote, and the deals negotiated between Google and large corporate outlets in the wake of the law's passing could negatively impact media diversity (FREEDOM HOUSE, 2022)[13].

1.3.11 *Online Safety Act 2021 (Cth)*

A aprovação do *Online Safety Act* 2021 trouxe mudanças significativas para a legislação australiana, de modo que os provedores de serviços online passam a ser responsáveis pela segurança das pessoas que utilizam seus serviços (AUSTRÁLIA, 2022e).

A nova lei amplia os poderes do *eSafety Commissioner,* estabece uma série de expectativas que deverão ser atendidas pelo provedores e exige que indústria desenvolva novos códigos de práticas para reprimir conteúdo ilegal e restrito (que compreende situações que envolvem abuso sexual, terrorismo, violência de alto impacto, nudez, entre outros).

Além disso, cria um esquema de abuso cibernético direcionado a adultos, amplia o esquema de *cyberbullying* direcionado a crianças, atualiza o esquema de abuso baseado em imagem e estabele um esquema de conteúdo online ilegal e restrito, que abarca conteúdos considerados "abomináveis", definidos de acordo com o *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act.*

De acordo com a lei, o esquema de abuso cibernético direcionado a adultos compreende todo tipo de comunicação online (comentários, postagens, e-mails, mensagens, memes, imagens e vídeos) que tenha como objetivo causar sérios danos psicológicos ou físicos. Além disso, a mensagem deve ser de algum modo ameaçadora, intimidadora, ofensiva ou assediante e deve ser dirigida a uma pessoa específica (que tenha 18 anos ou mais). Para caracterizar o abuso cibernético, ambos os critérios devem estar presentes. No entanto, é importante ressaltar que não entram nessa definição críticas negativas, opiniões fortes, brincadeiras ou danos à reputação, apenas aquilo que é considerado *"serious harm"* (AUSTRÁLIA, 2021b).

Já o esquema *cyberbullying* direcionado a crianças se refere a todo e qualquer tipo de comunicação online que seja seriamente ameaçadora, intimidadora, assediadora ou humilhante dirigida a uma pessoa menor de 18 anos. Para que haja uma investigação, também é necessário que o comentário também faça referência a uma criança em particular (AUSTRÁLIA, 2021c).

O esquema de abuso baseado em imagem, por sua vez, tenta coibir o compartilhamento sem o consentimento (ou a ameaça de divulgação) de uma

13 Tradução livre: "Os críticos disseram que o News Media Bargaining Code garante que as grandes corporações de notícias se beneficiem dos 'modelos sistemáticos de coleta e exploração de dados' que as plataformas digitais promovem, e os acordos negociados entre o Google e grandes veículos corporativos após a aprovação da lei podem impactar negativamente diversidade de mídia".

imagem íntima, com o objetivo de causar danos, humilhar ou constranger a pessoa retratada. Para isso, não importa a forma que a imagem tenha sido obtida, nem se foi compartilhada para pessoas específicas ou o público em geral, mas apenas que isso esteja sendo utilizado contra determinada pessoa (AUSTRÁLIA, 2021c).

Por último, o esquema de conteúdo online ilegal e restrito abrange materias classe 1 e classe 2, definidos de acordo com o Esquema Nacional de Classificação da Austrália[14]. Os materiais classe 1 compreendem conteúdos relacionado a sexo, drogas, crime, crueldade, violência ou situações consideradas "abomináveis"; ofensivo para um adulto "razoável" ou para um criança; ou que incite, promova ou instruia a prática de crimes. Já materiais classe 2 engloba conteúdos que são restritos a adultos, que inclui material sexualmente explícito (X18+) ou de alto impacto (R18+) que pode ser ofensivo para certos grupos (AUSTRÁLIA, 2021e). Ademais, o *eSafety Commissioner* tem o poder de solicitar ou exigir que um ISP bloqueie um material classificado como "abominável". As exceções dispostas na Divisão 2 da lei são semelhantes às definidas no código criminal (AUSTRÁLIA, 2021a).

Em todos os casos, para atrair a competência do *eSafety Commissioner* é necessário que o evento tenha ocorrido em um social media service, relevant electronic service ou em um designated internet service. O *"social media services"* (AUSTRÁLIA, 2021g) compreende serviços eletrônicos em que:

a) o único ou principal objetivo do serviço é permitir a interação social online entre 2 ou mais usuários finais;

b) permite que os usuários finais se conectem ou interajam com alguns ou todos os outros usuários finais;

c) permite que os usuários finais postem material no serviço;

d) outras condições (se houver) conforme estabelecido nas normas legislativas.

Já *"relevant electronic services"* (AUSTRÁLIA, 2021g) refere-se a

e) serviço que permite aos usuários finais se comunicarem, por meio de e-mail, com outros usuários finais;

f) serviço de mensagens instantâneas que permite aos usuários finais se comunicarem com outros usuários finais;

g) serviço de SMS que permite aos usuários finais se comunicarem com outros usuários finais;

h) serviço MMS que permite aos usuários finais se comunicarem com outros usuários finais;

i) serviço de bate-papo que permite que usuários finais se comuniquem com outros usuários finais;

j) serviço que permite aos usuários finais jogar jogos online com outros usuários finais;

k) serviço eletrônico especificado nas normas legislativas.

Por fim, o *"designated internet services"* (AUSTRÁLIA, 2021g) engloba

l) um serviço que permite aos usuários finais acessar um material através de um serviço de transporte pela Internet; ou

14 Esquema Nacional de Classificação da Austrália foi desenvolvido a partir de um acordo cooperativo entre o governo federal, dos estados e territórios para classificar publicações, filmes, séries de televisão e jogos de computador.

m) serviço que entrega materiais a pessoas que possuem equipamento adequado para recebê-lo quando a entrega do serviço é feita por meio de um serviço de transporte pela Internet, mas não inclui: i) serviço de mídia social; ou ii) serviço eletrônico relevante; ou iii) serviço de programa sob demanda; ou vi) serviço especificado na subseção (2); ou v) serviço isento (isto é, quando nenhum dos materiais do serviço estiver acessível ou seja entregue a um ou mais usuários finais na Austrália).

Além disso, o Ministro pode, por instrumento legislativo, especificar um ou mais serviços para efeitos deste último.

Ainda de acordo com a lei, provedores e usuários terão 24h para remover o conteúdo indicado, que poderá ser estendido a critério de *eSafety Commissioner* pelo mesmo. O não cumprimento da ordem de retirada pode resultar em multa de até AU $555.000 (US $396.000) para empresas e de AU $111.000 (US $79.100) para pessoas físicas. A lei também autoriza que o *eSafety Commissioner* impeça o download de aplicativos que violem a lei (FREEDOM HOUSE, 2022).

A lei também estabelece as chamadas *Basic Expectations of Online Safety* (BESO), ou seja, um conjunto de regras que buscam promover mais transparência e proatividade por parte dos provedores de serviços online, estabelecidas pelo Ministro de Comunicações por meio de resolução (AUSTRÁLIA, 2022d, p.3).

Além disso, há uma exigência para que a indústria desenvolva códigos de práticas, adotando medidas "razoáveis" e reprimindo práticas ilegais e nocivas às pessoas no ambiente online. Esses códigos serão obrigatórios para setores que oferecem serviços de distribuição de aplicativos, provedores de serviços de internet, mecanismos de busca, serviços de mensagens eletrônicas, fabricantes e fornecedores de equipamentos utilizados para o acesso de serviços online e pessoas que instalem e mantenham esses equipamentos (AUSTRÁLIA, 2022e).

O *Online Safety Act* 2021 é alvo de críticas por parte da sociedade civil, empresas de tecnologia e ativistas, que questionam os seus requisitos de remoção de conteúdo e alertam para o potencial efeito negativo da lei para grupos marginalizados, como profissionais do sexo, educadores sexuais, pessoas LGBTQIA+ e artistas (FREEDOM HOUSE, 2022).

1.4 Jurisprudência

Em 1975, o caso entre a *University of New South Wales vs Moorhouse* (AUSTRÁLIA, 1975a) foi fundamental para estabelecer os contornos do alcance da expressão "autorizar" da lei de propriedade intelectual. Na ocasião, a universidade foi acusada de infringir a lei de direitos autorais de diversos escritores, por ter disponibilizado uma fotocópia, sem nenhuma supervisão ou advertência quanto às regras de direitos autorais, ao lado de uma biblioteca, possibilitando que os estudantes pudessem facilmente reproduzir cópias de livros disponíveis no acervo. A partir desse caso, foram estabelecidas as regras do chamado *Moorhouse Test*, método utilizado para verificar se, no caso concreto, o provedor autorizou efetivamente a violação de direitos autorais por parte de seus usuários.

Em *Trkulja v Yahoo!* (AUSTRÁLIA, 2012c), a Suprema Corte de Victoria condenou o *Yahoo!*, com base na seção 22 (2), da Lei de Difamação de 2005, por hospedar um artigo de conteúdo ofensivo sobre a reputação do autor. Em 2009, o autor solicitou a retirada do conteúdo, mas o *Yahoo!* se recusou a tomar qualquer atitude sobre o caso, alegando que a indexação do artigo ao mecanismo de busca é feita de forma automatizada e sugeriu que ele falasse diretamente com os administradores do site onde o artigo foi compartilhado. O Tribunal, no entanto, considerou que a manutenção do conteúdo pelo buscador potencializou os danos à reputação do autor, sendo o *Yahoo!* condenado a pagar uma indenização ao reclamante.

Já em *Google Inc. v ACCC* (AUSTRÁLIA, 2013), a Suprema Corte entendeu que o provedor não era responsável pelos anúncios que apareciam nas páginas de resultados de pesquisa por hospedá-los em sua plataforma, uma vez que o conteúdo era produzido por terceiros e publicado automaticamente pelo *Google*. Nesse caso, exigiu-se a demonstração efetiva de que o provedor se "envolveu" ou "endossou" de alguma forma o conteúdo falso ou enganoso, levando o consumidor ao erro, o que os autores não conseguiram demonstrar. Conforme o *Report of Regulation of Digital Media and Intermediaries:*

> *The High Court here set a high threshold for liability: claiming actual wrongful conduct on the part of the defendant, rather than just awareness of said conduct. This therefore goes beyond an actual knowledge approach, requiring an active fault element from the intermediary* (OMOND et al, 2021, p. 35)[15].

Sendo irrelevante, portanto, se o Google sabia que o conteúdo era enganoso.

Em *Duffy v Google Inc.* (AUSTRALIA, 2015b), o Tribunal Pleno da Suprema Corte da Austrália do Sul considerou o Google responsável pela publicação de conteúdo difamatório, uma vez que a empresa tinha sido notificada pela reclamante em 2009, mas não tomou nenhuma atitude para cessar a divulgação do material. Dessa forma, o conteúdo difamatório continuou aparecendo no resumo do resultado na pesquisa, sendo disponibilizado hiperlinks para artigos com conteúdo difamatório hospedado em outros sites. O Google alegou divulgação inocente, privilégio qualificado, justificação e veracidade contextual, mas o Tribunal não acatou.

Em *Roadshow Films Pty Ltd v iiNet Ltd* (AUSTRÁLIA, 2012a), o Tribunal decidiu que o provedor não poderia ser responsabilizado pelas infrações de direitos autorais cometidas pelos assinantes da plataforma. Diante desse caso, foi proposta uma alteração na lei de direitos autorais através do Acordo de Livre Comércio Austrália-Coreia (KAFTA) 2014 (AUSTRÁLIA, 2014), com o objetivo de incentivar a cooperação entre provedores e proprietários para identificar essas violações (Chapter 13, Intellectual Property Rights, Article 13.5). Em *Pokémon v Redbubble* (AUSTRÁLIA, 2017a), o Tribunal considerou a *Redbubble Ltda* responsável pela violação de direitos autorais da *Pokémon Inc*, mesmo o provedor tendo adotado medidas de mitigação de dano após ser notificado.

Em outro caso interessante, conhecido como *X v Twitter Inc* (AUSTRÁLIA, 2017b),

15 Tradução livre: "O Supremo Tribunal estabeleceu aqui um alto limite para responsabilidade: reivindicar conduta ilícita real por parte do réu, em vez de apenas conhecimento da referida conduta. Isso, portanto, vai além de uma abordagem de conhecimento real, exigindo um elemento de falha ativa do intermediário".

a Suprema Corte de Nova Gales do Sul considerou que o Twitter deveria ter removido proativamente o conteúdo ofensivo postado por um troll que utilizou várias contas da plataforma para divulgar informações ofensivas sobre um autor não identificado. O Twitter tinha sido notificado e removeu o conteúdo, mas os ataques continuaram. O tribunal argumentou que a plataforma poderia ter bloqueado proativamente as novas ofensas mesmo sem novas notificações do autor.

Por fim, *Fairfax Media Publications v Voller* (AUSTRÁLIA, 2021f), um grupo de empresas que administravam várias páginas no Facebook foram consideradas responsáveis pelas postagens difamatórias publicadas. O tribunal considerou o grupo de empresas como "editoras" das páginas. Dessa forma, pouco importava a falta de conhecimento, que tinha sido alegada pelos réus na defesa, sobre os conteúdos que estavam sendo postados. Já que, segundo o tribunal, as rés participaram do processo editorial que tornou público e acessível para os demais (SLOAN, 2021).

1.5 Projetos de Leis

Em junho de 2021, foi aprovado o *Telecommunications Legislation Amendment (International Production Orders) Bill* que, para fins de segurança nacional, facilita o acesso do Estado a comunicações criptografadas. Em agosto de 2021, entrou em vigor o *Surveillance Legislation Amendment (Identify and Disrupt) Bill* que concede, entre outros poderes, a possibilidade de agências governamentais assumirem o controle das credenciais da contas eletrônicas de indivíduos na Internet para investigar e impedir crimes considerados "graves" (FREEDOM HOUSE, 2022).

Em fevereiro de 2022, após repercussão do caso *Fairfax Media Publications v Voller*, o Governo australiano encaminhou para o Parlamento o *Social Media (Anti-Trolling) Bill.* O projeto de lei determina que as plataformas devem fornecer dados como nome, endereço de e-mail e número de telefone de usuários que utilizam contas anônimas para difamar terceiros, sob pena de serem responsabilizadas pelos comentários supostamente ofensivos proferidos na plataforma (AUSTRÁLIA, 2022f).

De acordo com a *Freedom House* (2022):

> *Lawmakers and civil society organizations criticized the bill as 'grossly inadequate' to meet its stated purpose, citing the lack of provisions preventing online abuse or trolling practices and the bill's focus on empowering individuals to bring defamation lawsuits rather than pushing platforms to address online harms through design changes (FREEDOM HOUSE, 2022)*[16].

Até o momento, o *Social Media (Anti-Trolling) Bill* não foi aprovado pelo parlamento.

16 Tradução livre: "Os legisladores e as organizações da sociedade civil criticaram o projeto de lei como 'grosseiramente inadequado' para cumprir seu objetivo declarado, citando a falta de disposições que previnam o abuso online ou as práticas de trollagem e o foco do projeto de lei em capacitar os indivíduos a abrir processos por difamação, em vez de forçar as plataformas a lidar com os danos online por meio de alterações de design".

1.6 Discussões Atuais

Apesar de a Austrália ser considerada um país democrático, é possível notar um crescimento no número de leis que ampliam as obrigações dos provedores, aumentam as restrições na Internet, enfraquecem a criptografia, criando um estado de vigilância e monitoramento no país.

Especialistas apontam que as mudanças que vêm ocorrendo nos últimos anos podem causar prejuízos significativos para a liberdade de expressão e a privacidade dos cidadãos australianos, especialmente para aqueles que fazem parte de grupos mais vulneráveis, colocando em risco a manutenção da própria democracia no país.

A Austrália também não possui uma lei forte que proteja a privacidade e os dados pessoais dos cidadãos australianos. A constituição australiana também não fala sobre direito à privacidade. Contudo, infere-se a existência desse direito a partir de outras normas consuetudinárias. Apesar de alguns Estados e Territórios exigirem um certo nível de retenção e armazenamento de dados para setores específicos, a legislação federal australiana não apresenta requisitos gerais para a localização de dados pessoais (BAKER, 2023).

No *Privacy Act* 1988 (Cth), é possível encontrar, além das circunstâncias em que poderão ser utilizadas e a forma como serão coletadas e armazenadas, quais serão as informações consideradas "pessoais" que podem ser retidas pelo governo. Em outubro de 2021, o governo apresentou um documento para discussão, no qual sugeria alterações no *Privacy Act* 1988. O texto previa mudanças na definição de informações pessoais e estabelecia prerrogativas para que os cidadãos pudessem acionar a Justiça em caso de violação da lei (FREEDOM HOUSE, 2022).

O fenômeno da desinformação também é um dos desafios que o governo precisa lidar. Em fevereiro de a associação industrial sem fins lucrativos, o *Digital Industry Group Inc*., que defende os interesses da indústria de tecnologia na Austrália, em parceria com a ACMA, publicou um "Código de práticas para combater a desinformação no país", cabe a autoridade fiscalizar a aplicação das orientações do Código.

De acordo com o *Freedom House* (2022), o código desenvolvido:

> *outlines practices to label, demote, or remove certain categories of false information; to prioritize credible content including through fact-checking programs; and to enhance transparency reporting"*[17]*. Empresas como Twitter, Google, Facebook, Microsoft, Redbubble e TikTok "are among the platforms to have adopted the code, and have since started removing offending content, including on topics like the COVID-19 pandemic (FREEDOM HOUSE, 2022)*[18]*.*

17 Tradução livre: "descreve práticas para rotular, rebaixar ou remover certas categorias de informações falsas; priorizar conteúdo confiável, inclusive por meio de programas de verificação de fatos; e para melhorar os relatórios de transparência".

18 Tradução livre: "estão entre as plataformas que adotaram o código e, desde então, começaram a remover conteúdo ofensivo, inclusive sobre tópicos como a pandemia do COVID-19".

2 CANADÁ

2.1 Considerações iniciais

Atualmente, o Canadá não possui uma legislação específica para responsabilidade civil de intermediários, mas sim jurisprudência, projetos de Lei, documentos técnicos, acordos internacionais e discussões multissetoriais que caminham no sentido de regulamentar o tema.

Anteriormente às eleições federais de 2021, o Governo do Canadá emitiu um documento técnico, *"Technical Paper"*(CANADÁ, 2022c), para modernizar o Ato de Privacidade do Parlamento *(Privacy Act)* através do *Canadian Heritage*, propondo uma estrutura de regulação de plataformas focada em eliminar cinco tipos de conteúdos ilegais: pornografia, conteúdo terrorista, incitação à violência, discurso de ódio e compartilhamento não consensual de imagens íntimas.

O documento técnico faz menção ao Código Penal canadense e propõe que uma futura legislação seja instituída para regular conteúdos nocivos – esses conteúdos nocivos, por seu turno, precisam se encaixar nos tipos penais citados. Segundo o documento, a legislação, apesar de dever seguir o que preza o Código Penal canadense, poderá adaptá-lo no que for necessário para que esses tipos penais sejam aplicados dentro da realidade referida - isto é, de conteúdos postados em provedores de aplicação de Internet.

No módulo 1A: Novo quadro legislativo e regulamentar *(New legislative and regulatory framework)*, o documento do Governo deixa claro a primazia do Código Penal canadense sobre esse assunto no tópico de Aplicação 8 *(Application 8)* quando diz que a Lei deve fornecer definições para os cinco tipos de conteúdo nocivo de acordo com os conceitos definidos na Lei; e ainda que a Lei deve garantir que as definições sejam emprestadas do Código Penal, mas adaptadas ao contexto regulatório da Internet (CANADÁ, 2022c).

Dentre outras obrigações, os OCSP *(Online Communication Service Provider)*, ou Provedor de Serviços de Comunicação Online, como são chamados os provedores de aplicação no Canadá, precisariam responder a todas as notificações dos usuários que acusem um conteúdo de ser ilegal num prazo razoável, além de fornecer relatórios de transparência sobre o que motivou a retirada do conteúdo (e quais foram os conteúdos mais encontrados pela Plataforma).

Os provedores de aplicação também seriam cobrados para fornecer, com transparência, os termos de uso e de moderação de conteúdo para os usuários. O documento técnico do governo propõe, por exemplo:

a) Que os OCSP utilizem quaisquer medidas razoáveis, incluindo a utilização de sistemas automatizados, para identificar um conteúdo ofensivo propagado, tornando-o indisponível para qualquer pessoa que esteja dentro do Canadá;

b) Que os OCSP analisem toda e qualquer publicação que seja acusada por um usuário de conteúdo nocivo, e que essa análise seja feita num prazo razoável. O documento não deixa claro se um período razoável seria 24 horas ou mais, porém frisa que o OCSP precisa fornecer um espaço para que um usuário possa "denunciar" a publicação e que essa denúncia seja acompanhada de uma resposta formal;

c) Que seja criada uma Comissão de Segurança Digital *(Digital Safety Commissioner)* que, dentre outras obrigações, teria o dever de fiscalizar o cumprimento da futura legislação. Além disso, a Comissão teria o poder de impor penalidades às plataformas caso essas não cumpram a lei. A comissão, segundo o documento técnico, teria o poder de uma agência regulatória criada pelo próprio Governo, com a presença de profissionais de diversas áreas[19];

d) Que seja criado um regime de reclamações supervisionado pela Comissão, dando ao Comissário o poder de investigar, ouvir submissões e emitir uma decisão sobre a reclamação (WHITMORE; GUEST; OAKE, 2021).

Apesar de até o momento a legislação não ter sido criada e aprovada, o documento técnico do governo serviu de embasamento para alguns projetos de lei que tentam endereçar o discurso de ódio na Internet, como a Bill C-10 e a Bill C-11.

Quando se trata de jurisprudência, no Canadá, existem algumas decisões que apontam que as plataformas podem ser consideradas responsáveis por conteúdos postados por terceiros se esses conteúdos forem conteúdos difamatórios - a difamação é um tipo penal no Canadá. A jurisprudência será abordada em seguida neste relatório. Além da difamação, a responsabilidade de intermediários no Canadá se baseia ainda em alguns trechos da Lei de Direitos Autorais canadense, de 1985, trazida no tópico abaixo.

2.2 O arcabouço legal

2.2.1 *United States-Mexico-Canada Agreement*

O Canadá aderiu em 1º de julho de 2020 ao *United States-Mexico-Canada Agreement* (ESTADOS UNIDOS DA AMÉRICA, 2020), de 2018. Porém, como o acordo internacional ainda não foi convertido em leis domésticas pelo Canadá, sua aplicação ainda é incerta no país. A adesão do Canadá ao USMCA provocou uma discussão, entretanto, sobre a possibilidade de o CDA 30 ser aplicado na América do Norte como um todo, e não apenas nos Estados Unidos.

O Artigo 19.17 do Capítulo 19 do USMCA, requer que o Canadá ofereça um *safe harbour* para sistemas de serviço de computador, que aqui podem ser enxergados como os provedores de conexão, assim como aos intermediários – plataformas que possibilitam a publicação de conteúdo por terceiros.

Atualmente, como a Seção 230 dispõe que provedores de Internet não são responsabilizados por publicações de terceiros, os intermediários, tanto nos Estados Unidos, quanto no Canadá (e no México), através do USMCA, não são atores legítimos

19 A Comissão de Segurança Digital canadense é composta por profissionais da Academia, Sociedade Civil e do Governo (CANADIAN HERITAGE, 2020).

a serem responsabilizados civilmente por publicações feitas por usuários que utilizam esses serviços (no caso, os intermediários não serão responsabilizados no Canadá em razão do conjunto de legislações proveniente dos Estados Unidos [Seção 230] e do Acordo feito entre os três países citados).

Além disso, o acordo internacional dispõe, no Artigo 19.17.2, que nenhum provedor de conexão ou de aplicação será responsabilizado por conteúdo danoso provenientes de informações armazenadas, processadas ou transmitidas a não ser que esse provedor de conexão ou aplicação tenha ele próprio criado o conteúdo ou desenvolvido a informação.

2.2.2. *Copyright Act* (1985)

A Lei de Direitos Autorais canadense de 1985 (CANADÁ, 1985), apesar de ter sido escrita antes mesmo da disseminação de conteúdo online, ainda pode afetar a responsabilização de intermediários na Internet. Alguns pesquisadores criticam a influência que leis mais antigas têm em decisões que fazem parte de outro escopo e de realidade, como a da Internet e dos provedores de aplicação. Com relação à regulação de plataformas, a Lei de Direitos Autorais traz as seções 2.4(1)(b), 27 e 29 no escopo da legislação, que é utilizada como paralelo para a responsabilidade de intermediários atualmente. A Seção 2.4(1)(b) afirma que um intermediário não é responsável por infrações de direitos autorais simplesmente por fornecer os meios de telecomunicações necessários para que outros atores se comuniquem ou compartilhem conteúdos digitais.

O *Wilmap*, do *CIS-Stanford*, destaca o trecho anterior mencionado como um dos pontos principais em relação a responsabilização de intermediários trazido pelo *Copyright Act* (THE CENTER FOR INTERNET SOCIETY, 2017). As seções mencionadas são denominadas como Isenção de Transportadora Comum *(Common Carrier Exemption)* - ou seja, a seção segue a lógica de que um canal de televisão, por exemplo, não seja responsabilizado pelas propagandas de terceiros que veiculam em seu canal; ademais, que jornais e revistas não sejam responsabilizados por editoriais de opinião de terceiros que sejam veiculados em suas publicações. Assim, intermediários não poderiam ser responsabilizados por conteúdos postados por terceiros.

2.2.3. *Copyright Modernization Act* (2012)

A Lei de Direitos Autorais de 1985 foi alterada em 2012 pela Lei de Modernização de Direitos Autorais (CANADÁ, 2012). A Lei de Modernização de Direitos Autorais expande a isenção trazida pela Lei de Direitos Autorais de 1985 e legisla, em sua seção 31.1, que qualquer pessoa que esteja na posição de prestador de serviço relacionado a Internet e que forneça quaisquer meios necessários para a telecomunicação ou para a reprodução de conteúdo online, não pode ser considerada culpada por infringir os direitos autorais do conteúdo compartilhado, visto que essa seria somente um "provedor", ou facilitador do conteúdo. A Lei de Modernização de Direitos Autorais

oferece uma isenção mais abrangente do que a Lei de Direitos Autorais. Neste caso, a Lei de Modernização isenta os intermediários em quaisquer meios que estes utilizem para o compartilhamento de conteúdo, como, por exemplo, as redes sociais (STANFORD, 2017).

A Lei de Modernização de Direitos Autorais também inclui um sistema de *"notice and notice" p*elo qual o "dono" do meio de comunicação (o intermediário, a rede social) deve transmitir ao usuário (o terceiro) um aviso de violação recebido de um proprietário dos direitos autorais do conteúdo veiculado (CANADÁ, 2021c). Então, o caminho parte do próprio detentor do direito autoral: caso este verifique que algum conteúdo seu está sendo veiculado em alguma plataforma sem a sua autorização, deve escrever um aviso *(notice)*, em formato de formulário, de acordo com a seção 41.25 da Lei de Modernização de Direitos Autorais, e encaminhá-lo ao provedor, que não será obrigado a retirar o conteúdo, como em outros regimes (a exemplo do *Notice and Takedown*, aplicado na Alemanha). A única obrigação do intermediário é encaminhar o conteúdo ao terceiro - este, sim, terá a obrigação de retirar o conteúdo que viola direitos autorais.

A lei não especifica nenhuma outra ação a ser necessária para os intermediários, e a responsabilidade independe da remoção do conteúdo infrator - no caso, o intermediário só é responsável se não transmitir o aviso. Caso o intermediário receba o aviso escrito de acordo com o que prevê a Lei de Modernização (escrito, em formulário, indicando o conteúdo e o usuário que está compartilhando-o, entre outras especificidades definidas pelo 41.25[2] da Lei) e não encaminhe esse aviso para o terceiro identificado, poderá incorrer em multa que não ultrapasse 10 mil dólares mas que não seja inferior a 5 mil dólares, a depender da decisão da Corte. A multa é, portanto, a única penalidade em que incorre o intermediário.[20]

Por isso, a Lei de Modernização de Direitos Autorais do Canadá pode ser enxergada como uma versão canadense do *DMCA Takedown* (DMCA, 2022). Esse regime, como mencionado,é chamado de Regime de Aviso e Aviso (HEER, 2022) e entrou em vigor em 2 de janeiro de 2015 como parte da Lei de Modernização de Direitos Autorais do Canadá.

2.2.4 *Elections Modernization Act* (2018)

O Ato de Modernização das Eleições (CANADÁ, 2018) emendou o Ato de Eleições canadense de 2000 *(Canada Elections Act)* com algumas responsabilidades para as plataformas no sentido de prevenir o compartilhamento de desinformação no período eleitoral. Para a responsabilidade civil de intermediários, a norma é relevante à medida que traz, para esses, a responsabilidade de identificar quando uma publicação foi feita nas suas redes com intuito de publicizar ou fazer algum tipo de campanha eleitoral.

20 Lei de Modernização de Direitos Autorais, seção 41.26(3): *"Damages related to notices: (3) A claimant's only remedy against a person who fails to perform his or her obligations under subsection (1) is statutory damages in an amount that the court considers just, but not less than $5,000 and not more than $10,000.", em português: "Danos relacionados a notificações: (3) O único recurso do autor contra uma pessoa que não cumpre suas obrigações nos termos da subseção (1) é uma multa em valor que o tribunal considere justo, mas não inferior a $5.000 e não superior a $10.000".*

2.2.5 C-1.1: Ato de Quebec (2022)

O Ato de Quebec, *C-1.1: Act to establish a legal framework for information technology* (CANADÁ, 2022b), específico da província citada, teve sua primeira versão em 2001, mas sofreu diversas modificações e emendas com o passar dos anos, tendo a sua última versão datada de Setembro de 2022. A regulação concede imunidade aos intermediários em relação à responsabilidade por conteúdos postados por terceiros. De acordo com esta lei, as plataformas não teriam o dever de auto-regulação - como, por exemplo, o dever de ativamente procurar por conteúdos que infrinjam leis locais ou seus termos de uso (LAIDLAW, 2019). Em sua seção 22, a norma prevê que intermediários não são responsáveis por conteúdos postados por terceiros a menos que tenham ciência *(becoming aware)* de que um conteúdo ilícito foi postado. De acordo com essa previsão, paira uma ambiguidade em relação à responsabilidade quanto à identificação da informação ilícita por parte das plataformas. Segue:

> 22. *A service provider, acting as an intermediary, that provides document storage services on a communication network is not responsible for the activities engaged in by a service user with the use of documents stored by the service user or at the service user's request.*
> *However, the service provider may incur responsibility, particularly if, upon becoming aware that the documents are being used for an illicit activity, or of circumstances that make such a use apparent, the service provider does not act promptly to block access to the documents or otherwise prevent the pursuit of the activity."* (CANADÁ, 2022b).[21]

O Ato de Quebec exclui a obrigatoriedade de monitoramento de conteúdos ilícitos pelas plataformas e não restringe a aplicação de suas previsões a conteúdos difamatórios ou que violem os direitos autorais, mas sim abrange em suas disposições todos os conteúdos ilícitos que porventura venham a ser veiculados. Portanto, a ambiguidade lançada pode ser lida como intencional, já que a lei propõe uma espécie de safe harbour a intermediários.

2.3 Jurisprudências

A difamação como tipo penal canadense influenciou alguns julgamentos quanto à responsabilidade de intermediários - como nos casos *Carter v. B.C. Federation of Foster Parents* (CANADÁ, 2005), da província da Colúmbia Britânica, e *Baglow v. Smith (*CANADÁ, 2011), da província de Ontário.

No primeiro processo, a Corte considerou que as plataformas são responsáveis quando falham em remover conteúdo ofensivo difamatório contra um usuário. O segundo julgado seguiu a mesma lógica e declarou culpados "os operadores de

21 Em português: "22. O prestador de serviços, na qualidade de intermediário, que preste serviços de armazenamento de documentos em rede de comunicações não é responsável pelas atividades exercidas por um utente do serviço com a utilização de documentos armazenados pelo utente ou a seu pedido.
No entanto, o prestador de serviços pode incorrer em responsabilidade, especialmente se, ao tomar conhecimento de que os documentos estão a ser utilizados para uma atividade ilícita, ou de circunstâncias que tornam aparente tal uso, o prestador de serviços não agir prontamente para bloquear o acesso aos documentos ou caso contrário, impedir o exercício da atividade." (CANADÁ, 2022b).

mensagens online" por comentários difamatórios que haviam sido publicados numa postagem de terceiro. Outras duas decisões importantes dão uma pista sobre o caminho que as Cortes canadenses pretendem seguir, no que diz respeito à responsabilidade civil de intermediários - nessas duas decisões, assim como nas duas primeiras, nenhuma Corte decidiu que as plataformas não possuem nenhuma medida de responsabilidade sobre conteúdos postados por terceiros.

Em *Giustra v. Twitter Inc.* (CANADÁ, 2021a), um caso famoso no escopo de difamação de uma figura pública, o empresário Frank Giustra, que vive na província da Colúmbia Britânica, no Canadá, entrou com a ação contra o Twitter após diversos ataques recebidos na plataforma que tiveram alcance da mídia. Como resposta, o Twitter alegou que o caso deveria ser analisado na Califórnia, por ser a localização da sede da empresa. Porém, a parte acusadora apelou, visto que, se o caso fosse julgado nos EUA, seria julgado de acordo com a Primeira Emenda e a seção 230 do *Communications Decency Act* (CDA), portanto o Twitter não teria nenhuma responsabilização quanto ao conteúdo difamatório postado por terceiro.

A corte foi favorável ao requerente e ordenou que o caso permanecesse sob a jurisdição da Columbia Britânica, no Canadá. Um dos argumentos considerados para a decisão foi em relação à ausência de responsabilidade, caso a queixa fosse julgada na Califórnia, assim como a constatação sobre o local do delito *(locus delicti commissi)*, que aconteceu no Canadá, e suas consequências devido ao autor ser uma figura pública. Ademais, os tweets difamatórios foram majoritariamente acessados na província do Canadá, assim como o dano à reputação de Giustra, que também se deu na localização da Columbia Britânica.

A partir dessa decisão, a corte canadense abriu um precedente para que os cidadãos possam processar provedores de aplicação de Internet, como o Twitter, independente de onde seja a sede da empresa, contanto que haja operação em solo canadense e, ainda, que o caso (e seus efeitos) estejam vinculados ao local. Há, portanto, um debate sobre a competência, cuja doutrina não se apega às barreiras jurisdicionais quando se trata de assuntos envolvendo o ambiente da Internet. O caso específico de *Giustra vs Twitter* chegou ao fim em Janeiro de 2023, após anos de disputa: Giustra fez um acordo com o Twitter para que o processo fosse terminado, porém as condições do acordo ainda não foram reveladas publicamente. De comum acordo entre as duas partes, o caso foi finalizado no dia 06 de Janeiro de 2023 - alguns canais de reportagens tentaram contatar o autor do processo, porém nenhum desfecho foi revelado pelo seu advogado (CBC News, 2023).

Já no julgamento de *Lehouillier-Dumas v. Facebook inc* (CANADÁ, 2021b), a Corte canadense da província de Quebec rejeitou o argumento de que o Facebook possuía a obrigação de remover conteúdo potencialmente difamatório, sendo obrigado a remover apenas conteúdo ilegal ou conteúdo que tenha sido considerado difamatório pela Corte (e não apenas conteúdos meramente ofensivos ou desagradáveis).

Portanto, é de se entender que o Canadá ainda está caminhando para uma uniformização de decisões judiciais acerca da responsabilidade de intermediários, pois nenhuma legislação com foco apenas nesta matéria foi aprovada até o momento e decisões diferentes foram tomadas pelas Cortes em relação a diferentes queixas contra os provedores de aplicação - sendo tal variação constatada em diferentes províncias.

2.4 Projetos de lei

2.4.1 Bill C-10

Esse projeto de Lei foi extinto quando o Parlamento do Canadá se dissolveu, em meados de agosto de 2021, tendo passado apenas pela Câmara *(House of Commons)* e não pelo Senado[22]. Porém, seu texto foi amplamente criticado e recebeu muita atenção da mídia nacional e internacional quando proposto, e mais importante, serviu de base para o projeto de Lei seguinte chamado de Bill C-11 (CANADÁ, 2022a).

Basicamente, o referido projeto defendia que as plataformas de *streaming* de conteúdo, como o YouTube, concedessem parte de sua publicidade para conteúdos produzidos no Canadá, de forma a incentivar a produção e o consumo de conteúdo local.

Políticos de orientação liberal defenderam esse projeto com base nos outros meios alternativos de compartilhamento de conteúdo, como o jornal impresso, o rádio ou a televisão – que possuem, dentre outras, a obrigatoriedade de transmitir parte de seu conteúdo em produções locais.

Entretanto, o projeto de lei recebeu críticas de vários setores pois essa obrigatoriedade teria impactos na liberdade de expressão, por afetar a própria produção de conteúdo dos usuários, e na neutralidade da rede, pois os algoritmos de "organização" e visualização de conteúdo também seriam regulados pela Lei, especificamente pelo órgão administrativo, a CRTC – *Canadian Radio-Television and Telecommunications Comission* (LEWIS, 2018). No caso, conteúdos produzidos no Canadá deveriam ter preferência de exibição através dos mecanismos de busca das plataformas.

Uma das tentativas de regulação dos intermediários na Bill C-10 (CANADÁ, 2021d) surge a partir do contexto da propriedade intelectual de conteúdos veiculados pelas plataformas. De acordo com proposição da Lei, as plataformas seriam obrigadas, a partir dali, a identificar esses conteúdos e pagar uma porcentagem do lucro deles ao CRTC. Esse lucro deveria então ser convertido para a criação de mais conteúdo cultural canadense, como músicas, séries e filmes.

2.4.2 Bill C-11

Trata-se de projeto de lei posterior ao Bill C-10 que tramita, atualmente, no Parlamento do Canadá. Faz menção a alguns conteúdos já abordados anteriormente pela Bill C-10, porém com incidência apenas às companhias e empresas, e não ao usuário de plataformas de *streaming.*

O projeto de Lei defende que as empresas estrangeiras operem de acordo com as mesmas regulações das empresas canadenses e que sejam reguladas pelo órgão administrativo (CRTC). É, mais uma vez, uma tentativa de realizar uma emenda ao *Broadcasting Act canadense* - uma forma de:

22 Quando há a dissolução do Parlamento para eleições federais no Canadá todos os Projetos de Leis que ainda não foram aprovados são extintos (TOWNSEND, 2021).

> [...] garantir que os produtores independentes do Canadá tenham uma oportunidade justa de negociar com os compradores de conteúdo para possuir, controlar e monetizar a propriedade intelectual que eles desenvolvem e produzem (SCHMITZ, 2022).

A Bill C-11 faz parte de um projeto maior de regulação dos provedores de aplicação e das empresas de tecnologia no Canadá, visto que o tema da responsabilização de intermediários se refere apenas à primeira de três partes do texto.

Na parte três, a Bill C-11 visa resolver problemas relacionados ao compartilhamento de discurso de ódio e extremismo na Internet. No que se diz respeito aos pontos abordados na Bill C-10, o novo projeto de lei continua com a previsão de arrecadar parte do lucro de conteúdos em plataformas de *streaming* para o órgão administrativo CRTC, recebendo críticas no sentido de sua aplicação para produtores de conteúdo independentes como youtubers ou influencers.

A Bill C-11 faz referência a parte das espécies de provedores de aplicação sob o nome de *Online Communications Services* ou OCSs - que inclui o *Facebook, Instagram, Twitter* -, porém não inclui plataformas de mensageria instantânea e privada, como o *WhatsApp* ou o *Skype.* Na parte 3 de seu projeto, que se refere especialmente ao combate ao discurso de ódio, a Bill C-11 obriga os OCSs a "implementar medidas para identificar conteúdo prejudicial e responder a qualquer conteúdo sinalizado por qualquer usuário dentro de 24 horas" (GEIST, 2021).

O *Digital Safety Commissioner* (Comissão de Segurança Digital), já proposto pelo documento técnico canadense, aparece novamente na Bill C-11 como responsável por receber denúncias e pedidos de análise de conteúdo de usuários, de acordo com o interesse público. Quanto ao cenário das respostas provenientes do governo e da sociedade civil às legislações analisadas, em 2022 o governo do Canadá, através dos Ministros Pablo Rodriguez e David Lametti, anunciaram que irão criar um novo grupo multissetorial de especialistas em segurança online que, por sua vez, irá ajudar a desenvolver uma legislação sobre discurso de ódio online (CANADIAN HERITAGE, 2022).

Depois que o FCC – *U.S. Federal Communications Commission* fez um anúncio sobre a atual imunidade legal oferecida pela Seção 230 do CDA *(Communications Decency Act)* dos Estados Unidos, o Canadá, por ter assinado o USMCA, já abordado acima, e que seria obrigado a implementar a Seção 230 à sua atual jurisprudência e legislação, pode caminhar para outra perspectiva sobre a responsabilização civil de intermediários.

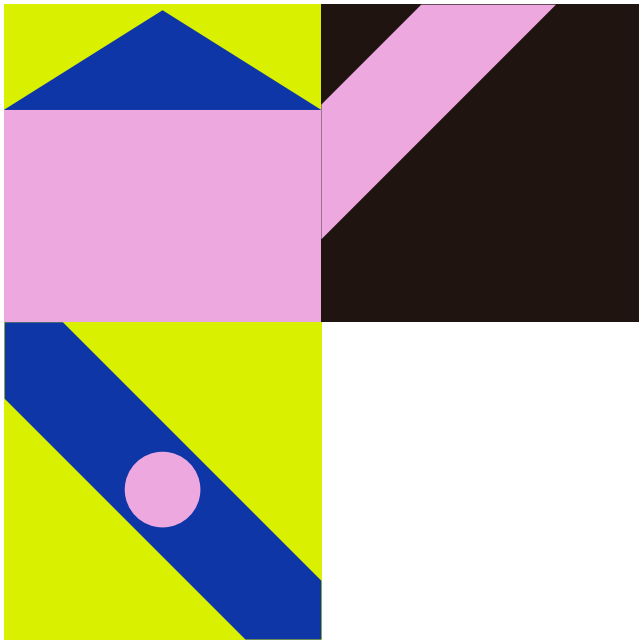
2.5 Discussões atuais

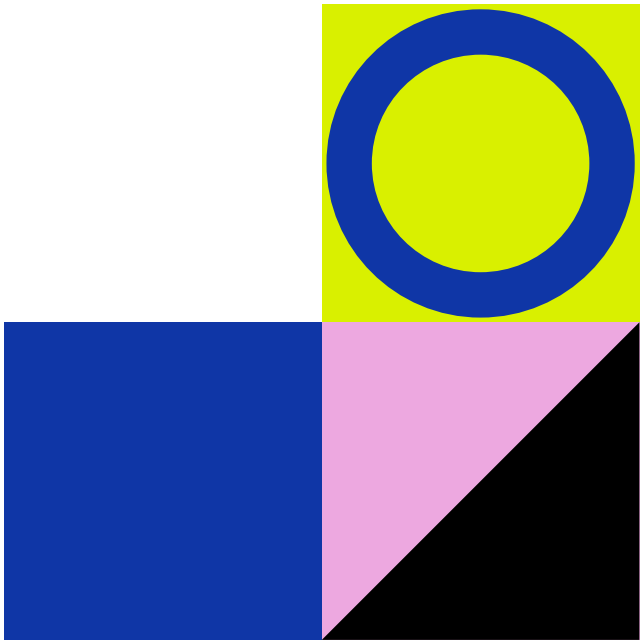
Parte da sociedade civil do Canadá tece dura críticas ao atual modelo de responsabilização adotado pelos Estados Unidos, visto que o CDA foi escrito em 1996 – numa época diferente, onde não se abordava as problemáticas do discurso de ódio, do extremismo e da desinformação impulsionadas através de plataformas digitais de maneira ampla.

O Canadá já balanceia a necessidade da liberdade de expressão (máxima), defendida pelos Estados Unidos no CDA, com a "necessidade que a sociedade possui por

limites razoáveis" (TSAI, 2020). Elementos como o discurso de ódio e a desinformação propagada através das redes sociais vêm abrindo margem para a discussão acerca da regulação das plataformas e da moderação de conteúdo. Com isso, setores da sociedade civil e academia reiteram a necessidade de um diálogo sobre a implementação do USMCA e do CDA americano no país. O Canadá deve seguir o CDA, por conta do USMCA, ou irá formular suas próprias regulações de acordo com a realidade do século XXI?

Uma possível saída que não seguir o CDA seria o endurecimento de leis criminais canadenses de modo a prevenir e responsabilizar intermediários por publicações que incitem a violência ou o terrorismo na Internet, por exemplo (KRISHNAMURTY; FJELD, 2020). O documento técnico do governo aborda essa opção como uma responsabilidade social que as plataformas devem ter, por transmitirem conteúdo - e consequentemente serem responsáveis por removerem conteúdos ilegais que porventura veiculem em suas mídias. Parte da sociedade civil que estuda a temática no país apoia que sejam implementadas políticas de *notice and takedown* no Canadá, semelhante ao que já acontece com publicações que violam direitos autorais, propriedade intelectual e mesmo o tipo penal da difamação. Ainda assim, a moderação de conteúdo legitimamente realizada pelas plataformas precisaria seguir os princípios mínimos da liberdade de expressão, devido processo, transparência e privacidade dos usuários (SOLOMUN; POLATAIKO; HAYES, 2021).





O SUL GLOBAL

3 INDONÉSIA

3.1. Considerações iniciais

A Indonésia é um país de maioria muçulmana (sunita), com um passado extremamente autoritário, que, recentemente, adotou a democracia como regime político. Com a quarta maior população do planeta, o país é considerado um dos 10 (dez) principais mercados do mundo, em número de usuários, para empresas de mídia social, dentre as quais estão *Alphabet Inc's, Youtube, TikTok, Twitter Inc e Meta*, sendo também um importante polo econômico para as empresas do setor (POTKIN; SULAIMAN, 2022).

No país, a estrutura da Internet é descentralizada. Contudo, o governo eventualmente impõe restrições de acesso, revelando que práticas autoritárias ainda permanecem presentes no dia a dia das pessoas. De acordo com a *Freedom House* (2021), o acesso à Internet foi comprometido durante eventos relacionados à independência de Papua Ocidental. Além disso, sites são frequentemente bloqueados por hospedar conteúdos proibidos, como pornográficos ou difamatórios, os que atentam contra a moral e os bons costumes, os que apresentam críticas ao governo e ao islã, dentre outros.

O país é acusado de assediar física e moralmente jornalistas, ativistas de direitos humanos e até mesmo usuários, sendo comum inclusive a prática de *doxing*, que consiste na divulgação de informações pessoais sem o consentimento com o objetivo de represália àqueles que se posicionam contra o governo (FREEDOM HOUSE, 2021).

Nos últimos anos, com o aumento das discussões em torno do problema da desinformação e discurso de ódio nas redes sociais, foram aprovadas duas normas administrativas: o Regulamento do Ministro de Comunicação e Informática N.º 5, de 2020 (RM5) e o Regulamento do Ministro de Comunicação e Informática N.º 10, de 2021 (RM10).

3.2 O Ministério de Comunicação e Tecnologia da Informação

Na Indonésia, a remoção e bloqueio de conteúdos considerados ilegais é atribuição do Ministério de Comunicação e Tecnologia da Informação *(Kominfo)*, sob o amparo da Lei de Informações e Transações Eletrônicas, com as diretrizes constantes no Regulamento Kominfo nº 19, de 2014.

O *Kominfo* é composto pela Direcção-Geral de Correios e Operações Informáticas ~~(PPI)~~ e pela Direcção-Geral de Aplicações Informáticas ~~*(Aptika)*~~. O primeiro órgão é responsável por supervisionar e regulamentar a atividade de provedores privados de telecomunicações, além de emitir licenças de provedores de serviços de Internet.

Enquanto o segundo gerencia os serviços de concessão de nomes de domínios para sites do governo e as atividades de remoção e bloqueio de conteúdo (FREEDOM HOUSE, 2021).

Em 2018, o *Kominfo* lançou um sistema rastreador chamado *"Cyber drone 9"* para detectar violações por conteúdo publicado. Uma equipe monitora o sistema e revisa o material sinalizado para bloqueio, determinando ao provedor a remoção, se couber. A partir de 2020, incorporou as funções do Órgão Regulador das Telecomunicações da Indonésia, dentre as quais a moderação de conteúdo (FREEDOM HOUSE, 2021).

Além do *Kominfo,* há outros órgãos governamentais que podem restringir acesso a conteúdo no país, como a Agência Nacional de Ciber e Criptografia, que tem o poder para filtrar e monitorar conteúdo online, nos casos em que houver interesse público e tiver como finalidade manutenção da ordem pública (FREEDOM HOUSE, 2021).

3.3 Arcabouço legal

3.3.1 Lei de Informações e Transações Eletrônicas

A Lei nº 11, de 2008, também conhecida como Lei de Informações e Transações Eletrônicas, é a principal legislação a disciplinar as transações eletrônicas no ambiente da Internet, abrangendo temáticas distintas, desde proteção de dados pessoais a natureza de conteúdo online e discurso de ódio (artigos 32 e 48).

Foi editada com o propósito de combater a pornografia, as mensagens de ódio religioso ou racial e a disseminação de notícias falsas, em resposta à preocupação da sociedade com os impactos negativos do crescimento dos acessos à Internet na país.

Uma das primeiras condenações sob a égide dessa lei foi a de Prita Mulyasari, em 2009, por haver compartilhado, por e-mail, a um grupo privado de amigos, críticas ao hospital onde foi vítima de erro de diagnóstico, quando internada para tratamento de saúde. Inicialmente, foi condenada a pena máxima prevista (06 (seis) anos de prisão e multa), como incurso no art. 27 da Lei nº 11/2008.

A grande repercussão do caso, a mobilização da sociedade e as discussões em torno dos limites à liberdade de expressão contribuíram para a sua absolvição, na mais alta instância do Poder Judiciário, a Suprema Corte[23].

O diploma legal sofreu alterações pela Lei nº 19, de 2016, que fortaleceram as bases legais para a remoção de conteúdo e o bloqueio do acesso à Internet no país.

23 http://indonesianlawadvisory.com/Case%20Prita.aspx

3.3.2 Regulamento do Ministro de Comunicação e Informática nº 5/2020

O Regulamento do Ministro de Comunicação e Informática nº 5/2020 (RM nº 5/2020) é um conjunto de preceitos e normas administrativas emitido pelo Ministério da Comunicação e Tecnologia da Informação da Indonésia *(Kominfo)*, que fortalece o controle do Estado sobre as plataformas de serviços online, por meio de regras que obrigam os Operadores de Sistemas Eletrônicos Privados, doravante referido como OSE Privado, a se submeterem ao ordenamento jurídico interno e cooperarem na suspensão de conteúdos publicados na internet. Foi promulgado em 24 de novembro de 2020.

A primeira alteração ocorreu em 2021, com a edição do Regulamento do Ministro de Comunicação e Informática nº 10, de 2021 (REPÚBLICA DA INDONÉSIA, 2021), que elevou à categoria de "negócio baseado em risco" as atividades desenvolvidas pelos OSEs Privados, trazendo novas obrigações, como a inscrição no *Indonesia's Online Single Submission System.* A medida é considerada uma exacerbação dos desafios à liberdade de expressão na Internet, por incrementar obrigações que expõem os provedores da Internet a penalidades excessivas pela não conformidade com as normas (ARTICLE 19, 2022).

O OSE Privado pode ser pessoa física ou jurídica, não governamental, que disponibiliza sistemas eletrônicos para usuários na Indonésia, mesmo que o controle técnico das operações ou a sede administrativa da instituição estejam em fora das linhas territoriais do país, o que alcança as empresas multinacionais.

Trata-se de conceito bastante amplo, abrangendo diversas categorias de plataformas de serviços online pela Internet, como as mídias sociais, os serviços de mensageria, de correio eletrônico, de compartilhamento de conteúdo, engenhos de busca, computação em nuvem, mercado digital, serviços financeiros, aplicativos de videochamadas, jogos, filmes, música, e outros que coletam, processam e analisam dados dos usuários para transações eletrônicas online[24].

Fortemente inspirado na *NetzDG alemã*[25], embora mais severo quanto à possível violação a direitos humanos, o RM5/2020 estabelece obrigações aos OSEs Privados, com vistas a facilitar a atuação do Estado no combate às violações ao Direito interno, perpetradas pela Internet. Nesse contexto, são obrigações impostas aos OSEs Privados, dentre outras:

a) Registro prévio em órgão governamental;
b) Nomeação de representante local;
c) Remoção de conteúdo e documentos proibidos;
d) Moderação de conteúdo.

---

24 Artigo 2º, (2) do RM5/2020 (REPÚBLICA DA INDONÉSIA, 2020).

25 A NetzDG é uma lei alemã, editada em 2017, que, dentre as normas, estabelece que as plataformas de mídia social,l com mais de 2 milhões de usuários, devem indicar representante local para atender requisições de autoridades públicas e promover a remoção de conteúdos manifestamente ilegais, no prazo de 24h, após a notificação, sob pena de receber multas draconianas. Seguindo a iniciativa da Alemanha, outros países instituíram leis ou estão em discussão a respeito. Venezuela, Austrália, Rússia, Índia, Quênia, Filipinas, Malásia são países que adotam modelo legal inspirado no alemão. O Brasil, desde 2020, discute o projeto de lei nº 2630/2020, também inspirado naquele. Essa legislação foi analisada no primeiro volume deste relatório, lançado em 2021.

3.3.2.1 Registro prévio

Antes de iniciar a atuação como OSE Privado, a entidade deve promover o seu registro junto ao Ministério da Comunicação e Tecnologia da Informação, que emite o respectivo certificado[26].

No momento do registro, o OSE Privado deve fornecer um conjunto de informações[27] que permitam ao Estado acesso aos sistemas e dados eletrônicos, de forma a garantir eficácia no processo de fiscalização e aplicação da lei.

As sanções relativas à violação do registro iniciam com um primeiro aviso, podendo culminar no bloqueio total de acesso à plataforma e a cassação da licença para operar no país[28].

3.3.2.2 Nomeação de representante local

Outra obrigação imposta pelo RM5/2020 é a nomeação de representante local para responder às ordens de remoção de conteúdo, atuar na moderação de conteúdo na rede e acesso a dados pessoais. Trata-se de requisito que expõe desnecessariamente a equipe local a responder, pessoalmente, por ações da empresa, além de dificultar a resistência da plataforma ao cumprimento de ordens arbitrárias ou ilegais (RODRIGUEZ, 2021; GLOBAL NETWORK INITIATIVE, 2021).

3.3.2.3 Remoção de conteúdo

É atribuição dos OSEs Privados a remoção de conteúdos e documentos eletrônicos considerados proibidos, tais como os que violam leis e regulamentos, os que atentam contra a "ordem pública" e os que causam "angústia à comunidade"[29], cabendo unicamente ao Ministério, uma autoridade não independente, a definição e abrangência desses dois últimos termos[30].

O termo "proibido", constante nos parágrafos (3) e (4) do Artigo 9º, tem alcance amplo, o que pode contribuir para interpretações que atendam a interesses do Estado, quando envolvido em conflitos, em oposição à garantia de direitos dos cidadãos. "Ordem pública" e "angústia da comunidade", por outro lado, são termos vagos e abrangentes,

---

26 Artigo 6º do RM5/2020 (REPÚBLICA DA INDONÉSIA, 2020).

27 De acordo com o Artigo 3º (4) do RM5/2020, devem ser fornecidas as seguintes informações: a) nome do Sistema Eletrônico; b) Setor de Sistemas Eletrônicos; c) localizador uniforme de recursos (URL); d) Sistema de nome de domínio e/ou endereços de servidor de Protocolo de Internet (IP); e) Descrição do modelo de negócio; f) breve descrição das funções do Sistema Eletrônico e dos processos de negócios do Sistema Eletrônico; g) informações sobre os Dados Pessoais processados; h) informações sobre o local de gerenciamento, processamento e/ou armazenamento de Sistemas Eletrônicos e Dados Eletrônicos; i) assumir o compromisso de fornecer acesso a sistemas e dados eletrônicos, a fim de assegurar a eficácia da fiscalização e aplicação da lei (REPÚBLICA DA INDONESIA, 2020).

28 Artigo 7º, (1) do RM5/2020 (REPÚBLICA DA INDONÉSIA, 2020).

29 Artigo 9º, (4) do RM5/2020 (REPÚBLICA DA INDONÉSIA, 2020).

30 Artigo 9º, (5) do RM5/2020 (REPÚBLICA DA INDONÉSIA, 2020).

impregnados de subjetividade, complexos e de difícil mensuração.

A "ordem pública" está relacionada ao grau de normalidade da vida social, sendo entendida como um conjunto de condições elementares, sem as quais não é possível a vida em comunidade civilizada. O termo "angústia da comunidade" é compatível com fatos que causem incômodo ao homem médio, à sociedade.

A manutenção da ordem pública pode servir de justificativa para limitar o exercício da liberdade de expressão (FELIPE, 2022). Alerta Rodriguez (2021) que, quaisquer restrições em prol da ordem pública devem estar previstas em lei (e não em normas administrativas, como no caso), além de serem necessárias, proporcionais e o último recurso para atingir o objetivo legítimo.

Em adendo, cabe ao OSE Privado remover qualquer publicação que possa "informar maneiras ou fornecer acesso" a documentos proibidos. Em termos práticos: um tutorial online que ensina a utilizar VPN para contornar o bloqueio de acesso poderá ser classificado como conteúdo a ser removido. Aliás, o próprio uso de uma VPN pode ser considerado conduta proibida.

De mais a mais, constitui obrigação dos OSEs Privados garantir que seu ambiente esteja livre de conteúdo e documentos considerados proibidos, comprometendo-se também a não disseminá-los[31], sob pena de ter bloqueado os acessos aos seus sistemas[32]. Para esse propósito, deve estabelecer modelo de governança, explicitando os direitos, deveres e limites de responsabilização dos usuários e da plataforma, em caso de violação às normas vigentes[33].

Na prática, essa obrigação imposta ao OSE Privado exige-lhe investimento em monitoramento frequente, com a adoção de filtros de conteúdo e outros mecanismos automatizados de identificação dos critérios que definem um conteúdo ou documento como proibido. A desnecessária e grave violação da privacidade de todos os usuários é uma das consequências imediatas dessa atividade.

A responsabilização dos OSEs Privados por conduta praticada por terceiros depende da observância e cumprimento das obrigações que lhe são impostas[34].

Em síntese, pode-se concluir que, na Indonésia, os OSEs Privados sempre serão responsabilizados por conduta de terceiros, pois, caso seja identificada uma violação, significa que a plataforma falhou em garantir que o seu ambiente esteja livre de conteúdos ou documentos proibidos, ou seja, fracassou na moderação de conteúdo.

Essas imposições trazem como consequências não apenas uma séria ameaça ao exercício do direito fundamental à liberdade de expressão dos indonésios, mas um grande desafio de conformidade para OSEs privados.

O efeito inibidor do discurso, também conhecido como *chilling effect*, certamente será um resultado do modelo posto pelo referido Regulamento, pois, para evitar sanções, ao primeiro sinal de proibição, o conteúdo é imediatamente retirado ou indisponibilizado, cabendo ao autor a defesa de sua permanência na Internet.

Outro desafio a ser enfrentado pelos OSEs Privados está relacionado às exigências de adequação da plataforma ao regime jurídico vigente. O dever de não permitir

31 Artigo 9º, (3) do RM5/2020 (REPÚBLICA DA INDONÉSIA, 2020).

32 Artigo 9º, (6) do RM5/2020 (REPÚBLICA DA INDONÉSIA, 2020).

33 Artigo 10 do RM5/2020 (REPÚBLICA DA INDONÉSIA, 2020).

34 Artigo 11 do RM5/2020 (REPÚBLICA DA INDONÉSIA, 2020).

conteúdos e documentos eletrônicos proibidos, por exemplo, obriga a moderação de conteúdo, que pode ocasionar graves violações aos direitos humanos, como o direito à privacidade e à liberdade de expressão.

E como ocorre, na prática, a remoção de conteúdo?

Cabe, unicamente, ao Ministério de Comunicação e Tecnologia da Informação definir que conteúdo ou documento são proibidos. A ausência de diálogo com a sociedade civil e a falta de transparência reforçam a natureza autoritária da governança da Internet no país, favorecendo manobras para conter a disseminação de discursos políticos e críticos ao Governo, de discussão de temas sensíveis, como a liberdade de expressão de públicos minoritários, como a população LGBTQIA+.

Ao chancelar um conteúdo ou documento como proibido, ao OSE Privado cabe apenas cumprir a obrigação de garantir que o seu ambiente não contenha nem facilite a disseminação.

No âmbito do Ministério, um funcionário é capacitado para exercer o cargo de Ministro do Bloqueio de Acesso, que é o responsável pela coordenação das atividades de controle de conteúdo e documentos online.

Os pedidos de bloqueio podem ser originários de órgãos de aplicação da lei, Tribunais, Ministério da Informação ou do público interessado.

Ao receber a solicitação, o Ministro comunica ao OSE Privado, que tem o exíguo prazo de 24 horas para cumprir, ou, se urgente, de 4 horas, como nos casos que envolvem terrorismo, pornografia infantil, ou conteúdo que cause incômodo à população ou que contribua com a pertubação da ordem pública.

Se o OSE privado, com exceção de um provedor de serviços de nuvem, descumprir a ordem, está sujeito a multas e, em caso extremo, ter os serviços bloqueados no país, mesmo que a natureza do conteúdo seja lícita, à luz do direito internacional.

3.4 O dilema das *BigTechs*

A incidência das normas jurídicas sobre as atividades desenvolvidas por empresas de tecnologia da informação no território indonésio, principalmente as *BigTechs* da Internet, suscita questionamentos quanto ao cumprimento das severas obrigações impostas pelo Estado, frente à responsabilidade das empresas no respeito aos direitos humanos.

Em consonância com os princípios gerais do Direito Internacional, a indústria da Internet tem a obrigação de respeitar os direitos humanos, o que inclui contribuir para que todas as pessoas possam, livremente, se expressar, independentemente de considerações de fronteiras, verbalmente ou por escrito, em forma impressa ou artística, ou por qualquer outro meio de sua escolha. Como não é direito absoluto[35], qualquer restrição ao seu exercício deve estar expressamente prevista em lei[36], e não em normas

35 Artigo 5, parágrafo 1 do Pacto Internacional sobre Direitos Civis e Políticos, adotado pela XXI Sessão da Assembléia-Geral das Nações Unidas, em 16 de dezembro de 1966.

36 Artigo 19 do Pacto Internacional sobre Direitos Civis e Políticos, ratificado como princípio geral em diversas Declarações Conjuntas em prol da liberdade de expressão na Internet, firmada entre organismos internacionais, por meio de seus representantes. Exemplos disponíveis em: https://www.oas.org/pt/cidh/expressao/showarticle.asp?artID=849&lID=4 e

administrativas, como os Regulamentos nº 5/2020 (REPÚBLICA DA INDONÉSIA, 2020) e nº 10/2021 (REPÚBLICA DA INDONÉSIA, 2021).

Assevera o Relator Especial das Nações Unidas (ONU) sobre a Liberdade de Opinião e Expressão que o Estado deve abster-se de exigir do setor privado a adoção de medidas que interfiram, desproporcionalmente, no exercício da liberdade de expressão. O que se observa, é que diversas normas constantes nos referidos Regulamentos indonésios afrontam, diretamente, normativas internacionais.

Quanto ao respeito à privacidade como direito fundamental, as disposições do Regulamento nº 5/2020 são potencialmente contrárias ao Artigo 12 da Declaração Universal dos Direitos Humanos e ao Artigo 17 do Pacto Internacional sobre Direitos Civis e Políticos, em especial as disposições que permitem às autoridades obter dados pessoais de OSEs privados. Essas preocupações são agravadas pela ausência de supervisão independente na obtenção de acesso a dados pessoais e pelo fato de que, na prática, os dados pessoais costumam ser mal utilizados, especialmente por agentes da lei (ACCESS NOW, 2021).

Esse aparato legislativo indonésio, adotado com o objetivo de enfrentamento ao discurso de ódio, pornografia e disseminação de notícias falsas, vem sofrendo duras críticas de vários setores da sociedade. Diversos documentos[37] foram endereçados às autoridades do país, pleiteando a revogação do RM nº 5/2020 (REPÚBLICA DA INDONÉSIA, 2020) e do RM nº 10/2021 (REPÚBLICA DA INDONÉSIA, 2021), sob alegação de grave violação aos direitos humanos.

Mesmo com regramentos autoritários, a sociedade se organiza para contribuir no enfrentamento a esses problemas. Similar ao *Sleeping Giants*[38], a Indonésia instituiu o *Masyarakat Anti Fitnah Indonesia* (Mafindo), iniciativa popular que permite que as próprias pessoas identifiquem e denunciem desinformação em plataformas digitais. Algumas empresas de tecnologia juntaram-se à iniciativa, em especial para evitar a proliferação de notícias falsas e desinformação, durante as eleições nacionais de 2019 (KAUR et al, 2018).

3.5 Jurisprudência

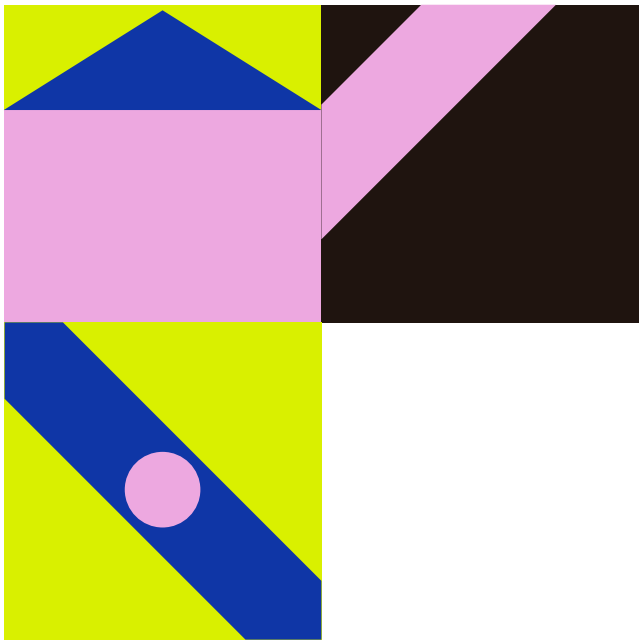
O direito à privacidade não se encontra expresso no texto constitucional (KAUR et al, 2018). No entanto, o Tribunal Constitucional, no caso *Anggara v Kominfo*, firmou a tese que é possível inferir o direito à privacidade do art. 28G (1) da Constituição, segundo o qual toda pessoa deve ter o direito à proteção de si mesmo, família, honra, dignidade e propriedade, e terá o direito de se sentir seguro e receber proteção contra a ameaça de medo de fazer ou não fazer algo que é um direito humano (REPÚBLICA DA INDONÉSIA, 1945).

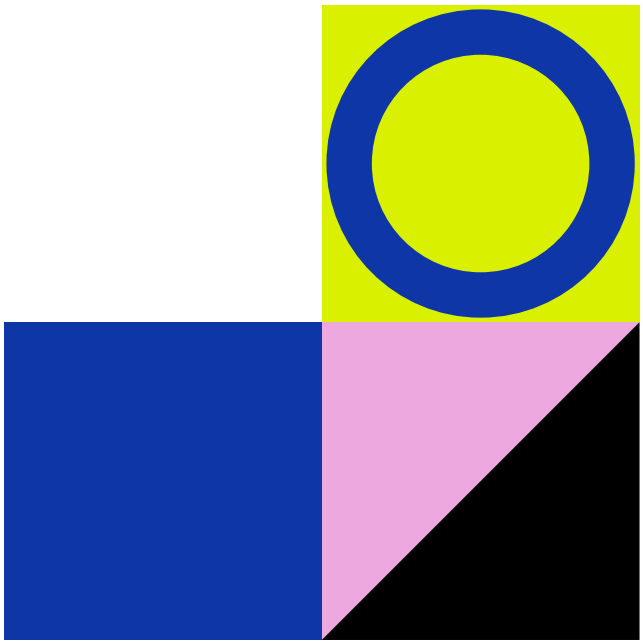
https://www.osce.org/files/f/documents/9/c/425282.pdf.

37 São exemplos: a Declaração Conjunta da Coalisão Global de Instituições Não-Governamentais (JOINT-STATEMENT, 2022); a Global Network Initiative (2021); a Declaração Conjunta conduzida pela Access Now (2021), com assinatura de mais de 25 (vinte e cinco) organizações não-Governamentais, em todo o mundo.

38 Movimento criado para denunciar sites que veiculam desinformação ou discurso de ódio, mencionando-os às grandes empresas que circulam publicidade nesses sites, para que deixem de receber financiamento das publicidades que os suportam.

Por outro lado, em 2021, o Tribunal Constitucional da Indonésia reconheceu a legalidade da decisão do governo da Indonésia de bloquear o acesso à internet durante os períodos de agitação social, na região de Papua. Segundo as autoridades, restringir o acesso à internet foi necessário na tentativa de prevenir a violência que poderia ter sido desencadeada pela rápida disseminação de desinformação online. Ativistas, como a Aliança Independente de Jornalistas da Indonésia, consideraram este um precedente perigoso para a liberdade na internet (COSTA; WIDIANTO, 2021).





4 RÚSSIA

4.1 Considerações iniciais

A Federação Russa é uma república semipresidencialista federal que tem o Presidente como chefe de Estado e o Primeiro-Ministro como chefe de Governo. A Assembleia da Federação Russa, que representa o Poder Legislativo, é bicameral, sendo constituída pela Duma do Estado e pelo Conselho da Federação.

A Duma do Estado é a Câmara Baixa, constituída por 450 (quatrocentos e cinquenta) deputados, eleitos para mandato de 05 (cinco) anos (POPOVA; ARNAUTOVICH, 2017). Compete-lhe a edição de leis constitucionais federais e leis federais[39], o controle das atividades do governo, a aprovação das candidaturas do primeiro-ministro, dos vice-primeiros-ministros e ministros federais, todos sob proposta do Presidente, a nomeação e destituição do chefe do Banco Central, Vice-Presidente da Câmara de Contas, Comissário para os Direitos Humanos, o anúncio de anistia, questões de cooperação parlamentar internacional[40].

O Conselho da Federação é a Câmara Alta da Assembleia Federal (POPOVA; ARNAUTOVICH, 2017). É composto por dois representantes de cada entidade da Federação Russa, sendo um representando a autoridade legislativa e o outro, a autoridade executiva. Ademais, são nomeados representantes, pelo Presidente da Federação Russa, em número que não exceda a 10% (dez por cento) dos membros das referidas entidades[41].

No Brasil, a Duma do Estado encontra equivalência à Câmara dos Deputados, e o Conselho de Federação, ao Senado Federal[42].

4.2 O (SUPER) órgão de controle e supervisão estatal

Roskomnadzor (RKN), abreviatura para Serviço Federal de Supervisão de Comunicações, Tecnologias da Informação e Comunicações de Massa (em russo: Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций)[43], é o órgão do executivo federal encarregado pela supervisão e controle estatal no campo das comunicações, tecnologias da informação (informática e telecomunicações) e das mídias de massa.

Foi instituído nos moldes atuais em maio de 2008, por meio da Resolução nº 419,

39 As leis constitucionais federais e as leis federais são a principal fonte de direito, com validade jurídica em toda a Federação Russa, regulando as relações sociais mais importantes.

40 http://duma.gov.ru/en/duma/about/

41 http://www.council.gov.ru/en/

42 ~~Para mais informações. Ver:~~ https://www.politize.com.br/russia-sistema-politico/

43 https://rkn.gov.ru/

"Sobre o Serviço Federal de Supervisão na Esfera das Telecomunicações, Tecnologias da Informação e Comunicação de Massa", de 6 de fevereiro de 2008.

As atribuições do órgão foram instituídas no Estatuto do *Roskomnadzor*, aprovado pelo Regulamento do Governo da Federação Russa Nº 228, de 16 de Março de 2009, "Sobre o Serviço Federal de Supervisão de Comunicações, Tecnologia da Informação e Mídia de Massa" (FEDERAÇÃO RUSSA, 2009).

No campo das comunicações[44], o RKN atua no sentido de regulamentar e implementar modelos de telecomunicações no país, assemelhando-se, aqui no Brasil, às atividades desenvolvidas pela Anatel (Agência Nacional de Telecomunicações).

Em 2008, RKN começou a emitir licenças para transmissão de rádio e televisão, serviços de comunicação, produção e reprodução de objetos audiovisuais, incluindo fonogramas. Ademais, assumiu o papel de coordenação dos serviços de radiofrequências e concursos na área dos serviços de comunicações (D.A. PROSHINA, 2022).

O controle da mídia também é questão que lhe diz respeito. Sob o argumento de preocupação com o desenvolvimento e saúde de crianças e adolescentes, no contexto dos acessos a conteúdos veiculados pelos meios de comunicação em massa, inclusive na Internet[45], o órgão, além de exercer censura sobre esses conteúdos, é o responsável pela acreditação de especialistas e organizações especializadas para o exame das produções[46]. Ademais, controla e supervisiona as transmissões em rádio e televisão, observando a conformidade com o ordenamento jurídico.

Relativamente à censura de conteúdos na Internet, dentre outras atribuições, cabe ao RKN fiscalizar as plataformas de comunicação, determinando a restrição ou remoção de conteúdos, independentemente de mandado judicial, cuja distribuição seja proibida na Federação Russa[47]. Identificado site ou domínio indesejado à Federação, é atribuição do RKN inseri-lo na "lista negra" de domínios e sites, mantendo-a atualizada[48].

Esses são apenas alguns exemplos dos poderes do RKN, estabelecidos pelo estatuto do órgão. No entanto, outras competências são criadas em normas específicas. Como exemplo, a Lei Federal nº 152-FZ, de 2006 (FEDERAÇÃO RUSSA, 2006b), que disciplina o tratamento de dados pessoais, autoriza o *Roskomnadzor* a bloquear sites ou limitar o processamento de dados pessoais, caso a empresa descumpra a obrigação de manter os dados pessoais dos cidadãos russos em território da Federação[49].

Embora a concessão de nomes de domínio na Internet seja uma atribuição do Centro de Coordenação do *Top-Level-Domain* (TLD) .RU e .РФ[50], o *Roskomnadzor* tem assento na instituição, representando o Estado russo, desde 3 de junho de 2020, o que facilita o controle sobre os domínios que fiscaliza.

44 Segundo o Estatuto do Roskomnadzor (FEDERAÇÃO RUSSA, 2009).

45 Item 5.5.1.6 do Estatuto do Roskomnadzor (FEDERAÇÃO RUSSA, 2009).

46 Item 5.1.6 do Estatuto do Roskomnadzor (FEDERAÇÃO RUSSA, 2009).

47 Item 5.1.7.1 do Estatuto do Roskomnadzor (FEDERAÇÃO RUSSA, 2009).

48 Item 5.1.7 do Estatuto do Roskomnadzor (FEDERAÇÃO RUSSA, 2009).

49 De acordo com o art. 23, parágrafo 4º da Lei Federal 152-FZ, de 2006 (FEDERAÇÃO RUSSA, 2006b).

50 O primeiro domínio cirílico nacional (*Internationalized country code Top-Level Domain* ou ccTLD) .РФ foi implementado em 12 de maio de 2010(https://cctld.ru/en/about/). Todos os nomes dos sites neste domínio deverão usar apenas letras do alfabeto cirílico, sendo este o quarto domínio no mundo e o primeiro no alfabeto cirílico a pertencer à categoria de domínios codificados para utilizar o sistema de escrita local, ao invés do alfabeto latino(https://www.iana.org/domains/reserved).

4.3 O arcabouço legal

4.3.1 O agente estrangeiro

É relevante considerar o conceito legal de agente estrangeiro enquanto estudamos o modelo de responsabilidade civil de intermediários, pela importância que o ambiente da Internet conquistou na difusão de informações, aliada às repercussões jurídicas para as empresas que se enquadram nesse requisito e atuam no território russo. Aliás, intermediários de informações, jornalistas, blogueiros e outras personalidades da Internet podem ser considerados agentes estrangeiros, por atuar em território russo e estar sob influência estrangeira.

A definição para agente estrangeiro foi introduzida, em 2012, pela Lei Federal nº 121-FZ, que regulamenta as atividades de organizações não comerciais, no exercício de funções de agente estrangeiro. Essa lei ficou conhecida como "Lei sobre Agentes Estrangeiros" e recebeu atualizações em 2014, 2016, 2019 (ROUDIK, 2021) e 2022.

Originalmente, era considerado agente estrangeiro qualquer organização não governamental ou pessoa jurídica russa que desempenhasse atividades político-partidárias no território da Federação Russa e recebesse financiamento externo, como de Estados estrangeiros, seus órgãos estatais, organizações internacionais, cidadãos estrangeiros, apátridas ou pessoas autorizadas por eles[51].

Mantendo esses dois critérios (atuar em território russo e receber financiamento do exterior), ao longo da última década, observa-se a inserção de novas entidades ao instituto e a adoção de penalidades mais rigorosas.

Em 2016, foram incluídas as organizações não comerciais (exceto partidos políticos) que realizassem atividades políticas[52]. Em novembro de 2017, a mídia estrangeira. Em dezembro de 2019, alcançou pessoas jurídicas e organizações não governamentais russas que trabalhassem com mídia ou divulgassem conteúdos em veículos de comunicação em massa[53], e pessoas físicas, como jornalistas e blogueiros, que compartilham esses conteúdos a um círculo ilimitado de pessoas, inclusive na Internet[54].

A partir de Julho de 2022, para ser considerado agente estrangeiro, é suficiente estar sob influência estrangeira[55].

Os agentes estrangeiros estão sujeitos a registro especial, obrigações específicas e monitoramento pelo Governo.

---

51 Artigo 2, parágrafo 2 da Lei Federal nº 121-FZ, de 2012 (FEDERAÇÃO RUSSA, 2012).

52 São exemplos de atividades políticas: atividades estatais, da proteção do sistema constitucional, federalismo, proteção da soberania e integridade territorial, estado de direito, segurança pública, defesa nacional, política externa, desenvolvimento social, econômico e nacional, desenvolvimento do sistema político, atividades do Estado e das autoridades locais, ou direitos humanos, com a finalidade de influenciar a política do Estado, a estrutura das autoridades estaduais e locais, ou suas decisões e ações. Ficam excluídas do âmbito da "atividade política" as do domínio da ciência, cultura, artes, cuidados de saúde, prevenção de doenças e proteção da saúde, segurança social, proteção da maternidade e da infância, apoio social às pessoas com deficiência, promoção de um estilo de vida saudável, bem-estar físico e esportivo, proteção da flora e fauna, atividades beneficentes (COUNCIL OF EUROPE, 2021).

53 Nos termos da lei federal Nº 426-FZ, de 2 dezembro de 2019, que alterou a Lei Federal nº 2124-1, de 27 de dezembro de 1991, sobre Mídia de Massa, e a Lei Federal nº 149-FZ, de 27 de julho de 2006 (FEDERAÇÃO RUSSA, 2006a).

54 De acordo com o Artigo 1 da Lei nº 426-FZ, de 2019, que alterou o Artigo 6 da Lei sobre mídias de massa.

55 Artigo 1, parágrafo 1 da Lei Federal Nº 255-FZ, de 14 de julho de 2022 (FEDERAÇÃO RUSSA, 2022a).

O primeiro requisito exigido para atuar como agente estrangeiro é o registro prévio[56], junto ao Ministério da Justiça. Nessa etapa, as entidades repassam diversas informações, como natureza das atividades desenvolvidas, responsável local, fontes de receitas, dentre outras.

Uma vez registrado, o agente estrangeiro deve observar um conjunto de obrigações legais que, na sua maioria, são de natureza financeira e tributária. São exemplos:

a) informar, trimestralmente, à autoridade estatal de registro sobre a aplicação do financiamento recebido do exterior;

b) se pessoa física, divulgar, semestralmente, relatório de atividades e descrição do uso dos recursos recebidos de fontes estrangeiras (COUNCIL OF EUROPE, 2021).

c) rotular as publicações e outros materiais, inclusive conteúdo online (como tweets individuais, postagens em redes sociais etc), com a referência de que os materiais foram produzidos e/ou distribuídos por indivíduo ou organização, desempenhando funções de agente estrangeiro[57];

d) para produções audiovisuais, o anúncio de que os materiais foram produzidos por um agente estrangeiro deve ter, no máximo, 15 segundos e ser veiculado no início da apresentação e no início de cada novo segmento de transmissão, após os intervalos comerciais[58].

Ao Estado compete a fiscalização e o controle do cumprimento dessas obrigações legais, cabendo-lhe realizar auditorias anuais[59] e, se constatadas irregularidades, aplicar as penalidades cabíveis, que podem culminar em suspensão das atividades, por 06 (seis) meses[60].

Importantes mudanças foram introduzidas no Código de Infrações Administrativas e no Código Penal, desde o ano de 2019. A título de exemplo, violação à lei do agente estrangeiro sujeita o cidadão comum a multas de até 100.000 Rublos (R$ 8.400,00), o funcionário público a 200.000 Rublos (R$ 16.800,00) e de até 5 milhões de rublos (R$ 420.000,00)[61], para pessoas jurídicas[62].

Em específico para pessoas físicas que atuam como agente estrangeiro, constitui crime deixar de apresentar os documentos necessários ao seu registro ou abster-se de cumprir as obrigações previstas na respectiva lei, caso já tenha sido responsabilizado administrativamente pelas mesmas condutas, por duas vezes ao ano[63]. Se essa pessoa coleta intencionalmente informações de natureza técnico-militar, estarão sujeitos a

---

56 O registro de pessoas físicas rotuladas como "agentes estrangeiros" segue o estabelecido na Lei Federal Nº 481-FZ, de 30 dez 2020.

57 Artigo 2, parágrafo 4, da Lei Federal nº 121-FZ (FEDERAÇÃO RUSSA, 2012); Artigo 251, parte 8, alterado pela Lei Federal nº 426-FZ, 2019 (FEDERAÇÃO RUSSA, 2019a); Ordem Roskomnadzor nº 124, de 23 de setembro de 2020.

58 Ordem Roskomnadzor nº 124, de 23 de setembro de 2020.

59 Artigo 2, parágrafo 5(a) da Lei Federal nº 121-FZ (FEDERAÇÃO RUSSA, 2012).

60 Artigo 2, parágrafo 5(zh) da Lei Federal nº 121-FZ (FEDERAÇÃO RUSSA, 2012).

61 Valores em Real, convertidos do Rublo russo, com base no câmbio do dia 21 set 2022, em: https://www.google.com/finance/.

62 O Artigo 1º da Lei Federal nº 443-FZ, de 2019 (FEDERAÇÃO RUSSA, 2019c), introduziu alterações ao Código de Infrações Administrativas.

63 A pena prevista é: multa no valor de até 300 mil rublos, ou no valor do salário ou salário, ou qualquer outra renda do condenado, por um período de até dois anos, ou por trabalhos obrigatórios por um período de até 480 horas, ou por trabalho corretivo por um período de até dois anos, ou por privação de liberdade pelo mesmo período (Artigo 330.1 Parágrafos 1 e 2 do Código Penal da Federação Russa (FEDERAÇÃO RUSSA, 1996), alterado pela Lei Federal nº 582-FZ, de 29 de dezembro de 2022).

penas mais severas[64], caso não se subsume a outros tipos penais mais graves.

Punições rigorosas a pessoas físicas representam, nitidamente, a intenção do Governo em controlar os conteúdos que circulam na Internet, bem como em criar mecanismos que facilitem a perseguição política a opositores, a jornalistas e suas fontes, ou apenas aos que compartilham esses conteúdos em suas redes sociais.

Organismos internacionais, notadamente o Conselho da Europa, advertiram para as consequências dessas medidas no exercício da liberdade de expressão, condenando-as por meio de pronunciamento e pareceres oficiais[65], pleiteando a revogação do status de agente estrangeiro a pessoa física (COUNCIL OF EUROPE, 2021).

Em 2014, o Tribunal Constitucional da Federação Russa julgou improcedente ação proposta pelo Comissariado de Direitos Humanos da Rússia, que defendia constituir violação de direitos e liberdades individuais as penalidades administrativas impostas a organização não governamental que recebia financiamento de fontes estrangeiras, para promover suas funções estatutárias.

No caso em concreto, uma certa organização não governamental foi punida por ter promovido eventos de cunho político, com recurso recebido do exterior, sem prévio registro como agente estrangeiro. Pela ação proposta, a designação como agente estrangeiro estigmatiza a instituição, infringindo-lhe direito de personalidade. Em decisão, o Tribunal entendeu que, o fato de uma organização estar registrada como agente estrangeiro, não interfere na sua imagem perante à sociedade nem tampouco causa preconceito às autoridades estatais (Tribunal Constitucional da Federação Russa, Decisão nº 10-P de 8 de abril de 2014) (FEDERAÇÃO RUSSA, 2014b).

4.3.2 Proteção de dados pessoais

O disciplinamento sobre a proteção de dados pessoais na Federação Russa é previsto, em sua maioria, pelas Lei Federal Nº 152-FZ, de 27 de julho de 2006 (FEDERAÇÃO RUSSA, 2006b) e Lei Federal Nº 149-FZ, de 27 de julho de 2006 (FEDERAÇÃO RUSSA, 2006a). Em termos gerais, o modelo legal está alinhado a padrões internacionais, como os previstos na Convenção de Estrasburgo, de 28 de janeiro de 1981, ratificada pela Rússia em 2005 (BUZKO; AGATEEV, 2022).

A privacidade e os dados pessoais recebem proteção constitucional, conforme dispõem os artigos 23 e 24 da Magna Carta da Rússia. Nos termos legais, é proibido coleta, conservação, utilização e divulgação de informações sobre a vida privada de uma pessoa, sem o seu consentimento (FEDERAÇÃO RUSSA, 1993).

Outras normas jurídicas também disciplinam o assunto, como o Código do

64 A pena prevista é: multa no valor de até 300 mil rublos, ou no valor do salário ou salário, ou qualquer outra renda do condenado por um período de até dois anos, ou por trabalhos obrigatórios por um período de até a 480 horas, ou por trabalho forçado por um período de até cinco anos, ou por privação de liberdade pelo mesmo período (Artigo 330.1 Parágrafo 3 do Código Penal da Federação Russa (FEDERAÇÃO RUSSA, 1996), alterado pela Lei Federal nº 582-FZ, de 29 de dezembro de 2022).

65 Comissário para os Direitos Humanos do Conselho da Europa (https://rm.coe.int/opinion-of-the-commissioner-for-human-rights-on-the-legislation-of-the/16806da5b2; e https://rm.coe.int/opinion-of-the-commissioner-for-human-rights-on-the-legislation-and-pr/16806da772); opinion of the European Commission for Democracy through Law ("the Venice Commission"): https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2014)-025-e.

Trabalho[66], a lei sobre segredos comerciais[67], a lei de segurança sobre infraestruturas críticas de informações[68], o código de infrações administrativas[69].

Como no Brasil, abrange o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado[70].

Para fins legais, dados pessoais é definido como qualquer informação relacionada direta ou indiretamente a uma pessoa física específica ou identificável (Artigo 3 parágrafo 1 da Lei Federal 152-FZ, de 2006), tais como apelido, nome próprio, patronímico, ano e local de nascimento, endereço, família, informações sobre a profissão, e-mail e qualquer outra informação capaz de identificá-lo[71]. A transferência de dados pessoais para terceiros, em desconformidade com a lei, sujeita à responsabilidade administrativa e criminal.

Ao longo de sua vigência, a lei de proteção de dados pessoais russa foi alterada por 27 (vinte e sete) novas leis, como: Lei Federal Nº 242-FZ, de 14 de julho de 2014 (FEDERAÇÃO RUSSA, 2014a), Lei Federal Nº 123-FZ de 24 de abril de 2020, Lei Federal nº 331-FZ de 2 de julho de 2021.

Outras normas, embora não a modifiquem diretamente, impõem obrigações ou estabelecem sanções relacionadas ao escopo de sua aplicação. São exemplos a Lei Federal Nº 236-FZ, de 1º de julho de 2021, também conhecida como a Lei do Desembarque, e a Lei Federal Nº 259-FZ, de 14 de julho de 2022, que altera o Código de Ofensas Administrativas da Federação Russa, impondo sanções mais severas a diversas infrações, inclusive no âmbito da proteção de dados pessoais.

São obrigações impostas a empresas estrangeiras que tratam dados pessoais de cidadãos russos:

a) notificar o *Roskomnadzor* sobre a localização dos dados pessoais;

b) publicar política de tratamento de dados pessoais;

c) nomear representante local;

d) informar ao *Roskomnadzor* sobre vazamentos de dados pessoais de usuários russos.

Cooperar com o *Roskomnadzor* não é uma alternativa, mas uma obrigação das empresas que pretendem processar dados pessoais na Rússia, especialmente quando relativos a cidadãos do país (PAVLOV, 2020).

O descumprimento aos requisitos impostos autoriza o *Roskomnadzor* a bloquear sites ou limitar o processamento de dados pessoais[72], além de aplicar penalidades administrativas aos altos executivos da empresa (diretor geral ou CEO)[73]

Em setembro de 2021, o *Roskomnadzor* implantou o Centro de Assistência Jurídica ao Cidadão no Ambiente Digital da Empresa Unitária Estadual Federal para atender, gratuitamente, vítimas de violações a dados pessoais, com repercussões financeiras. Desde a sua criação, mais de mil pessoas já foram atendidas (ROSKOMNADZOR, 2022).

66 Capítulo 14 da Lei Federal nº 197-FZ, de 30 de dezembro de 2001.

67 Lei Federal nº 98-FZ, de 26 de julho de 2004, sobre Segredos Comerciais.

68 Lei Federal nº 187-FZ, de 26 July 2017, sobre segurança de infraestrutura crítica de informações.

69 Lei Federal nº 195-FZ, sobre o Código de Ofensas Administrativas.

70 Artigo 1, parágrafo 1 da Lei Federal 152-FZ, de 2006 (FEDERAÇÃO RUSSA, 2006b).

71 Artigo 8 e Artigo 9 da Lei Federal 152-FZ, de 2006 (FEDERAÇÃO RUSSA, 2006b).

72 Segundo Artigo 23, parte 4º da Lei Federal nº 152-FZ, de 2006 (FEDERAÇÃO RUSSA, 2006b).

73 De acordo com o Código de Ofensas Administrativas da Federação Russa.

4.3.3 Localização de dados

A localização de dados é a prática de manter os dados na jurisdição onde foram coletados. Na Rússia, é obrigação das empresas, inclusive as estrangeiras, garantir que o tratamento de dados pessoais de cidadãos russos seja realizado em território da Federação Russa[74], sob pena de bloqueio das operações[75], concomitante a imposição de multas à empresa e aos altos executivos (*Chief Executive Officer* - CEO). A rede social Linkedin foi a primeira plataforma a ser condenada por violação à lei de localização de dados[76] (PAVLOV, 2020).

As incertezas sobre os limites e abrangência da lei pairam entre os interessados, como se é lícito armazenar cópias dos dados pessoais fora do país, criptografá-los, dentre outras questões (GEVORGYAN, 2017).

Os países que adotam esse tipo de medida argumentam que elas são fundamentais para a soberania digital e a segurança cibernética de seus cidadãos (RIBEIRO; BELOTTI, 2022).

2.2.3.4 A lei do Desembarque

A Lei Federal Nº 236-FZ, de 01 de julho de 2021, "Sobre as Atividades de Estrangeiros na Rede de Informação e Telecomunicações da Internet no Território da Federação Russa" (FEDERAÇÃO RUSSA, 2021), também conhecida como Lei do Desembarque, foi instituída com o objetivo de garantir a incidência das normativas russas a empresas e profissionais estrangeiros[77], quando em operação na infraestrutura de telecomunicações e/ou oferecendo serviços de Internet, no território russo[78]. Entrou em vigor, integralmente, em 1º de janeiro de 2022.

Concomitante à imposição de outras medidas, a Lei do Desembarque é adotada num cenário político empenhado em fortalecer a soberania digital russa e aumentar o controle do Estado sobre as atividades estrangeiras na área de tecnologia da informação.

Nesse sentido, a lei incide sobre:

a) empresas estrangeiras de Internet, incluindo as que oferecem serviços de mensageria e mídias sociais, que atendem, diariamente, pelo menos 500.000 (quinhentos mil) usuários na Rússia[79], e o fazem cumprindo, pelo menos, um dos

74 O artigo 2º da Lei Federal Nº 242-FZ, de 21 de julho de 2014, "Sobre Alterações a Certos Atos Legislativos da Federação Russa para Esclarecimento do Processamento de Dados Pessoais em Redes de Informação e Telecomunicações" (FEDERAÇÃO RUSSA, 2014a), alterou a Lei Nº 152-FZ, de 2006 (FEDERAÇÃO RUSSA, 2006b), introduzindo o princípio da localização de dados, segundo o qual os operadores devem garantir que o processamento de dados pessoais de cidadãos russos seja realizado em servidores e bancos de dados localizados em território da Federação Russa, alcançando, seus efeitos, empresas estrangeiras, quando envolvidas no processamento de dados pessoais de cidadãos russos.

75 Artigo 23, parágrafo 4º da Lei Federal nº 152-FZ, de 2006.

76 https://www.bbc.com/news/technology-38014501; http://ultimosfatos.com.br/?p=11605; https://g1.globo.com/tecnologia/noticia/2016/11/russia-bloqueia-rede-social-linkedin.html

77 Pessoas jurídicas estrangeiras, organizações estrangeiras que não sejam pessoas jurídicas, cidadãos estrangeiros, apátridas (Parágrafo 1 do Artigo 1º da Lei Federal nº 236-FZ, de 2021).

78 Artigo 2 da Lei Federal Nº 236-FZ, de 2021 (FEDERAÇÃO RUSSA, 2021).

79 Em razão da abrangência dos termos legais postos, é possível a incidência da lei sobre plataformas de pequeno ou médio porte (BANKOVSKIY et al, 2021).

seguintes requisitos: oferecem serviços em russo ou outros idiomas da Federação Russa; divulgam publicidade direcionada a clientes na Rússia; processam dados pessoais de clientes da Rússia; recebem fundos de pessoas físicas ou jurídicas russas[80];

b) entidades estrangeiras, atuando como intermediárias de informações, como: provedores de hospedagem; provedor de aplicação; administradores de recursos de publicidade destinada a usuários russos[81], e

c) indivíduo estrangeiro responsável pela organização e distribuição de publicidade na Internet, direcionada a consumidores russos ou que atuam na produção e divulgação de conteúdos[82], como blogueiros, streamers, e outras personalidades da Internet (CHELYSHKOV; IVANENKO, 2021).

Cabe ao ***Roskomnadzor*** determinar quais empresas se enquadram no segundo critério, com base em uma metodologia especial a ser estabelecida[83], bem como manter, em seu site oficial, a lista dessas empresas e indivíduos[84].

São obrigações impostas[85]:

a) disponibilizar formulários eletrônicos para interagir com cidadãos e organizações russas;

b) registrar conta pessoal no site oficial do RKN para facilitar a comunicação com órgãos estaduais, e

c) estabelecer sucursal, escritório de representação, ou entidade legal independente, no território da Federação Russa, que represente seus interesses e cumpra as decisões de Tribunais e órgãos estatais, incluindo a remoção de conteúdos. Por essa razão, ficou conhecida, aqui no Ocidente, como Lei do Desembarque.

Esse rol de obrigações é meramente exemplificativo, sendo as atividades dessas empresas reguladas também por outras leis e normativas vigentes, inclusive algumas já abordadas anteriormente.

Os efeitos da lei atingem, principalmente, as redes sociais, os serviços de mensageria, de audiovisuais, jogos online, motores de busca, mercados digitais, estabelecendo amplos poderes das autoridades russas sobre instituições e indivíduos estrangeiros que atuam nessa área (BANKOVSKIY et al, 2021; RICHTER, 2021).

Em caso de descumprimento de obrigações, a empresa estrangeira estará sujeita a sanções que podem culminar no bloqueio total aos recursos oferecidos, cabendo ao RKN a sua aplicação[86]. A partir de 1º de janeiro de 2023, por força da Lei Federal Nº 259-FZ, de julho de 2022 (FEDERAÇÃO RUSSA, 2022b), outras condutas passaram a ser penalizadas, como a desídia de *BigTechs* da Internet na entrega de informações requeridas pelo RKN, à recusa de instalar software que registre o número de usuários do aplicativo, ao descumprimento da obrigação de constituir representação local, ou ainda que ignorem a proibição de coletar dados pessoais de cidadãos russos[87].

80 Parágrafo 1 do Artigo 4º da Lei Federal Nº 236-FZ, de 2021 (FEDERAÇÃO RUSSA, 2021).
81 Parágrafo 2 do Artigo 4º da Lei Federal Nº 236-FZ, de 2021 (FEDERAÇÃO RUSSA, 2021).
82 Parágrafo 2 do Artigo 4º da Lei Federal Nº 236-FZ, de 2021 (FEDERAÇÃO RUSSA, 2021).
83 Parágrafo 3 do Artigo 4º da Lei Federal Nº 236-FZ, de 2021 (FEDERAÇÃO RUSSA, 2021).
84 Artigo 8º da Lei Federal Nº 236-FZ, de 2021 (FEDERAÇÃO RUSSA, 2021).
85 Artigo 5º da Lei Federal Nº 236-FZ, de 2021 (FEDERAÇÃO RUSSA, 2021).
86 Artigo 9 da Lei Federal Nº 236-FZ, de 2021 (FEDERAÇÃO RUSSA, 2021).
87 Artigo 19.5.2 do Código de Ofensas Administrativas da Federação Russa, inserido pela reforma.

4.3.5 As leis das *Fake News*

O enfrentamento às notícias falsas é aparelhado por um conjunto de leis federais que ficou conhecido como Leis das *Fake News*, sendo a primeira a Lei Federal nº 31-FZ, de 18 de março de 2019 (FEDERAÇÃO RUSSA, 2019b), e as mais recentes as Lei Federal nº 277-FZ, de julho de 2022 (FEDERAÇÃO RUSSA, 2022c), Lei Federal nº 32-FZ, de 4 de março de 2022 (FEDERAÇÃO RUSSA, 2022e) e Lei Federal nº 31-FZ, de 4 de março de 2022 (FEDERAÇÃO RUSSA, 2022d), promulgadas durante a invasão russa à Ucrânia, provocando a saída de várias empresas do país.

Os dispositivos proíbem as chamadas notícias falsas, cuja descrição engloba um conjunto abrangente de condutas, eivado de lacunas e imprecisões jurídicas. São exemplos a difusão de informações contendo convocações para motins em massa, atividades extremistas, participação em eventos de públicos; de informações destinadas a desacreditar o uso das Forças Armadas para a proteção dos interesses do país e de seus cidadãos; de materiais informativos de uma organização não governamental estrangeira ou internacional cujas atividades são reconhecidas como indesejáveis no território da Federação Russa; de publicações que visem perturbar o processo eleitoral; dentre outras[88].

Nesse sentido, investigações jornalísticas sobre temas que desagradar o Governo, como corrupção, ou quaisquer discussões online (não apenas em sites de mídia, mas simplesmente em redes sociais) que tratem de eventos de interesse público ainda não confirmados no momento da publicação, podem ser reprimidos, com base nas Leis das Notícias Falsas (BARATA; DAIRBEKOV, 2019a).

O *Roskomnadzor* pode determinar, extrajudicialmente, a remoção imediata ou o bloqueio de acesso ao conteúdo indesejado, sob pena de responsabilização do intermediário de informações, seja pessoa física ou jurídica, podendo, neste último, a sanção alcançar altos executivos da empresa ou o representante em território russo[89]. Em caso de reincidência, o acesso ao recurso pode ser suspenso em definitivo, irrevogavelmente[90].

88 Artigo 15.3 da Lei Federal nº 149-FZ, de 2006 (FEDERAÇÃO RUSSA, 2006a), com alterações posteriores.

89 Parágrafos 2, 3 e 4 do artigo 15.3 da Lei Federal nº 149-FZ, de 2006 (FEDERAÇÃO RUSSA, 2006a).

90 Artigo 15.3-2 da Lei Federal nº 149-FZ, de 2006 (FEDERAÇÃO RUSSA, 2006a), introduzido pela Lei Federal nº 277-FZ de 14 de julho de 2022 (FEDERAÇÃO RUSSA, 2022c).

4.4 A responsabilidade civil dos intermediários de informações

4.4.1 Visão geral

Não é por acaso que esta seção aparece em derradeiro, no contexto russo do direito digital. Parte considerável das consequências por violação às normas jurídicas tratadas acima culmina em responsabilização civil dos intermediários de informações, sem olvidar as sanções administrativas e penais pertinentes.

Por muito tempo, a Internet russa permaneceu relativamente livre de censura, com uma abordagem liberal e sem que o Estado expressasse interesse em sua regulamentação, mesmo quando as emissoras de televisão e jornais impressos do país submetiam-se a normas cada vez mais rígidas e restritivas (BIRNBAUM, 2014; HOVYADINOV, 2020). Nesse contexto, insere-se também a regulamentação da responsabilidade de intermediários.

Foi apenas em 2006, que a Lei da Informação introduziu uma abordagem semelhante à da União Europeia, isentando os intermediários tecnológicos de responsabilidade por ações de terceiros na transmissão, armazenamento e facilitação do acesso à informação (HOVYADINOV, 2020).

Atualmente, a matéria é disciplinada pela Parte Quatro do Código Civil (FEDERAÇÃO RUSSA, 2006c) e pela Lei Federal N° 149-FZ, de 27 de julho de 2006 (FEDERAÇÃO RUSSA, 2006a), detalhadas a seguir.

4.4.2 A Lei da Informação

A Lei Federal N° 149-FZ, de 27 de julho de 2006 (FEDERAÇÃO RUSSA, 2006a), Sobre Informação, Tecnologias da Informação e Segurança da Informação, também conhecida como Lei da Informação, é a norma jurídica que estabelece as regras gerais de uso e operação das tecnologias da informação[91]. Desde a sua edição, sofreu diversas alterações[92], sendo a última em 14 de julho de 2022, com a Lei Federal Nº 325-FZ.

As normas estão distribuídas em 18 (dezoito) artigos, reservado o 17º para a responsabilidade por delitos relativos à tecnologia da informação. A derradeira atualização, especificamente do artigo 17, foi realizada pela Lei Federal nº 530-FZ, de 30 de dezembro de 2020, que acrescentou o parágrafo 5.

Em linhas gerais, os intermediários de informações não serão civilmente responsabilizados por danos causados, em razão de conteúdos de terceiros, se, durante a transmissão da mensagem, o provedor de serviços não realize qualquer modificação

91 Exceto proteção de dados pessoais, direitos autorais, inteligência artificial, sendo-lhes destinadas legislações específicas.

92 Foram 57 (cinquenta e sete) alterações, sendo a primeira em 2010, com a Lei Federal Nº 227-FZ (http://www.consultant.ru/document/cons_doc_LAW_61798/).

no conteúdo e, em se tratando de provedor de hospedagem ou de provedor de conexão, desconheciam ou não tinham como saber a natureza ilegal do conteúdo[93].

Quando o conteúdo ilícito é divulgado em redes sociais, as vítimas da infração podem pleitear, em juízo, indenização a título de danos morais, proteção da honra, dignidade e reputação empresarial[94].

Em caso de publicações que violem direitos autorais, o provedor de hospedagem, o operador de telecomunicações e o proprietário do site não serão responsabilizados, perante os titulares de direitos autorais e usuários, por restringir o acesso ou remover o conteúdo, se atuarem conforme a lei[95].

Em se tratando de dados pessoais biométricos, a ofensa às regras de tratamento, inclusive quanto à confiabilidade no Sistema Unificado de Identificação e Autenticação e/ou no Sistema Biométrico Unificado[96], pode ensejar em responsabilização disciplinar, civil, penal e administrativa. O sujeito lesado por incorreções nesses sistemas, conexas ou não com o uso indevido dessas informações, pode exercer o direito à indenização por danos morais, proteção da honra, dignidade e reputação empresarial[97], desde que não tenha contribuído para a violação da confidencialidade dos dados nem descumprido os requisitos de proteção de informações estabelecidos pela legislação da Federação Russa, se a adoção dessas medidas e o cumprimento de tais requisitos constituem deveres dessa pessoa[98].

Essa é a regra geral posta na Lei de Informações.

No entanto, caso o intermediário de informações deixe de cumprir determinação do RKN[99], no sentido de bloquear ou restringir acesso a determinado conteúdo[100], ou demore a fornecer as informações requeridas pelo órgão, ou entregue-as erradas, deliberadamente, dificultando a identificação de usuário, sendo mais grave se estrangeiro, estará sujeito a responder civil e administrativamente, sendo as multas administrativas majoradas, a partir de 1º de janeiro de 2023, com a entrada em vigor da Lei Federal Nº 259-FZ, de julho de 2022 (FEDERAÇÃO RUSSA, 2022b).

A mesma lei também estabelece punição aos operadores de mecanismos de busca, que também são intermediários de informações, caso deixem de marcar, nos resultados de pesquisa, recursos estrangeiros que violam a legislação do país[101], bem como descumpram decisão do RKN, no sentido de ocultar resultados de pesquisa[102],

---

93 Artigo 17 Parágrafo 3 da Lei Federal nº 149-FZ, de 2006 (FEDERAÇÃO RUSSA, 2006a).

94 Artigo 17 Parágrafo 5 da Lei Federal nº 149-FZ, de 2006 (FEDERAÇÃO RUSSA, 2006a), introduzido pela Lei Federal nº 530-FZ ,de 30 de dezembro de 2020.

95 Artigo 4 da Lei Federal nº 149-FZ, de 2006 (FEDERAÇÃO RUSSA, 2006a).

96 O Artigo 14.1 trata sobre a aplicação de tecnologias de informação com o propósito de identificar pessoas (introduzido pela Lei Federal nº 482-FZ de 31 de dezembro de 2017 e alterado pela Lei Federal nº 479-FZ de 29 de dezembro de 2020).

97 Parágrafo 1 do do Artigo 17 da Lei Federal nº 149-FZ, de 2006 (FEDERAÇÃO RUSSA, 2006a).

98 Parágrafo 2 do do Artigo 17 da Lei Federal nº 149-FZ, de 2006 (FEDERAÇÃO RUSSA, 2006a).

99 As medidas cautelares e as decisões judiciais são encaminhadas para o RKN, que providencia o cumprimento pelos intermediários de informações.

100 A título de exemplo, o valor máximo da multa administrativa aplicada à pessoa jurídica passou de 800 mil para 4 milhões de rublos, conforme alterações impostas pela Lei Federal Nº 259-FZ, de julho de 2022 (FEDERAÇÃO RUSSA, 2022b).

101 Parágrafo 5 do art. 13.40 do Código de Ofensas Administrativas da Federação Russa, incluído pela reforma.

102 Parágrafo 6 do art. 13.40 do Código de Ofensas Administrativas da Federação Russa, incluído pela reforma.

aumentando o valor das multas administrativas aplicadas aos cidadãos, funcionários e pessoas jurídicas, em caso de reincidência[103].

4.4.3 O Código Civil da Federação Russa

O Código Civil da Federação Russa, que é a principal fonte de direito civil, é composto por quatro partes, que entraram em vigor em tempos diferentes.

A primeira parte, que trata das disposições gerais, apresentando os conceitos legais para os institutos tratados pelo Código, foi promulgada pela Duma Estatal em 1994 e entrou em vigor em 1995.

A segunda parte, que trata do direito das obrigações, entrou em vigor em 1996.

A terceira parte, com o direito das sucessões, entrou em vigor em 2002. Ademais, dispõe sobre princípios básicos, como a inviolabilidade da propriedade privada, liberdade contratual, livre exercício dos direitos civis, proteção jurídica dos direitos civis.

A quarta parte, que é a de interesse para o tema analisado neste Relatório, traz as normas jurídicas atinentes à propriedade intelectual e, nesse contexto, delineia a responsabilidade dos intermediários tecnológicos. Foi sancionada em 18 de dezembro de 2006 e entrou em vigor em 1º de janeiro de 2008 (FEDERAÇÃO RUSSA, 2006c).

Em resumo, tem-se:

Parte 1: Seção I: Disposições gerais; Seção II: Propriedade e outros interesses de propriedade; Seção III: A parte geral da lei de obrigações

Parte 2: Seção IV: Tipos específicos de obrigações

Parte 3: Seção V: Direito sucessório; Seção VI: Direito privado internacional

Parte 4: Seção VII: O direito aos produtos da atividade intelectual e meios de individualização.

Ao contrário da maioria dos códigos civis europeus e do brasileiro, o direito de família é disciplinado em legislação apartada. A última alteração no código civil russo ocorreu em 07 de outubro de 2022, pela Lei Federal nº 386-FZ.

4.4.4 Os intermediários de informações

A prática judicial, ao longo dos anos, vem evidenciado insegurança na conceituação dos vários tipos de intermediários de informações, conforme as atividades desenvolvidas, bem como quais podem ser responsabilizadas por violação de direito autoral (BUROVA, 2017; BARATA; DAIRBEKOV, 2019b; LORENZ, 2020).

No contexto da proteção à propriedade intelectual, o artigo 1253.1 do Código Civil[104] alude a conceitos e características da responsabilidade do intermediário de informações.

103 Parágrafo 7 do art. 13.40 do Código de Ofensas Administrativas da Federação Russa, incluído pela reforma.

104 Introduzido pela Lei Federal nº 187-FZ, de 02 de julho de 2013.

Pelo conceito jurídico legal, são intermediários de informações[105] todas as entidades, pessoas físicas ou jurídicas que:

a) Transmitem conteúdo através de uma rede de informações e telecomunicações, inclusive a Internet;

b) Oferecem recursos que possibilitam a publicação de conteúdo em rede de informações e telecomunicações, ou fornecem informações necessárias para acessá-los ou obtê-los;

c) Permitem o acesso ao conteúdo através de tais redes de informação e telecomunicações.Originariamente, enquanto os termos da lei eram discutidos, presumia-se a existência de apenas dois tipos de intermediários: o operador de telecomunicações e o provedor de hospedagem (BUROVA, 2017).

Denomina-se operador de telecomunicações a pessoa jurídica ou empresário individual que fornece serviços de comunicação, inclusive à Internet, com base em licença apropriada[106]. Provedor de hospedagem é uma entidade que oferece serviços baseados em poder computacional para publicação de informações em sistema conectado à Internet[107].

Antes da introdução do referido conceito legal, decisões judiciais foram proferidas no sentido de isentar de responsabilidade o intermediário de informações que desempenhava funções meramente técnicas, sem interferir no conteúdo que veiculava. A esse respeito, Burova (2017) destaca a decisão do Presidium do Supremo Tribunal de Arbitragem da Federação Russa nº 10962/08, de 23 de dezembro de 2008, no caso nº A40-6440/07-5-68, que inocentou provedor de hospedagem, em processo que apurava ofensa a direito exclusivo de reprodução e disponibilização de obras na Internet, acatando a tese de que, a mera disponibilização e manutenção do equipamento ao assinante, atividade puramente técnica, isenta de responsabilidade o provedor, pois ele não selecionou o destinatário, não iniciou a transmissão nem interferiu na integridade da informação.

Vários escritos[108] evidenciam a dificuldade para enquadrar, no conceito legal, os modelos existentes, no mundo técnico. Por vezes, é comum se amparar em experiências estrangeiras para criar um padrão conceitual, apoiado nas características dos serviços prestados (BUROVA, 2017).

Em termos gerais, decisões judiciais vêm classificando como intermediários de informações as seguintes entidade:

a) registradores de nomes de domínio (Resolução do Tribunal de Direitos de Propriedade Intelectual de 12.08.2016 nº C01-1000/2015 no processo nº A40-52455/2015);

b) administradores de nomes de domínio (Resolução do Tribunal de Direitos de Propriedade Intelectual de 16 de novembro de 2016 nº C01–959/2016 no caso nº A49–121/2016);

c) proprietários de sites, incluindo proprietários de redes sociais e de

105 Artigo 1253.1, parágrafo 1 do Código Civil (FEDERAÇÃO RUSSA, 2006c).

106 Parágrafo 12 do artigo 2 da Lei Federal nº 126, de 2003, a Lei das Comunicações.

107 Parágrafo 18 do artigo 2 da Lei Federal n° 149-FZ, de 2006 (FEDERAÇÃO RUSSA, 2006a).

108 Exemplos: Burova (2017), BARATA; DAIRBEKOV (2019b), Lorez (2020).

compartilhamento de arquivos da Internet (Resolução do Tribunal de Propriedade Intelectual de 07 de setembro de 2016 nº C01-704/2016 no caso nº A60-54898/2015, julgamento do Tribunal de Direitos de Propriedade Intelectual de 24 de abril de 2015 nº C01-251/2015 em processo nº A40-150342/2013);

d) serviços de busca (decisão do Tribunal de Direitos de Propriedade Intelectual de 15.12.2015 nº C01–491/2013 no caso nº A40–118705/2013);

e) operadoras de telecomunicações (decisão da Décima Terceira Arbitragem Tribunal de Recurso de 13.10.2016 N 13AP-21128/2016, 13AP-22544/2016 no caso N A56–88112/2015);

f) serviços de publicidade contextual (decretado sentença do Tribunal de Direitos de Propriedade Intelectual de 12 de setembro de 2014 nº C01-823/2014 no caso nº A40-145068/2013).

Observa-se, no entanto, a falta de uniformidade nas decisões judiciais. Cita-se, por exemplo, o entendimento em torno dos administradores e dos registradores de domínio[109]. Embora não haja unanimidade, predomina a compreensão de que ambos são considerados intermediários de informações. Os administradores do domínio, na acepção do artigo 1253.1 do Código Civil (FEDERAÇÃO RUSSA, 2006c), são considerados intermediários de informações, pois possibilitam a publicação de material ou informações por terceiros[110]. Quanto aos registradores de nomes de domínio, embora os Tribunais reconheçam-nos como intermediários de informação, não podem ser responsabilizados por conteúdos publicados em páginas cuja transmissão é realizada por meio desses nomes de domínio

Os proprietários de sites podem ser considerados intermediários de informações. Em contenda envolvendo a empresa VKontakte, entendeu o Tribunal que o site de mesmo nome, na URL www.vk.com, é um intermediários de informações, pois fornece aos usuários o serviço de criação de páginas pessoais e a publicação de conteúdos, como textos, vídeos, gravações de áudio, documentos, fotografias.

Os mecanismos de busca também são considerados intermediários de informação. De acordo com o parágrafo 20 do artigo 2 da Lei de Informação, um engenho de busca é um sistema de informação que, a pedido do usuário, pesquisa na Internet informações sobre determinado conteúdo, constantes em sites de terceiros, fornecendo ao usuário o índice para acessá-las. No entanto, não são responsáveis por atos de violação de direitos autorais praticados por seus usuários. Esse foi o entendimento no caso envolvendo o Tracksflow.com, serviço de busca de arquivos de música[111].

As atividades de intermediação na rede são qualificadas de acordo com os seguintes critérios (LORENZ; 2020):

a) a natureza técnica do serviço prestado;

---

109 O administrador de domínio é quem utiliza e administra o nome de domínio constante no respectivo Registro. O Registrador de domínio é a pessoa jurídica credenciada pelo Coordenador para o registo de nomes de domínio no .RU e /ou domínios .РФ, ou seja, inserir no Registro informações sobre o nome de domínio, seu administrador e outras informações e pertinentes.

110 Resolução do Tribunal de Direitos de Propriedade Intelectual de 30 de setembro de 2015 Nº C01-653/2015 no caso No. A56-77036/2013.

111 Resolução do Tribunal de Propriedade Intelectual de 15 de dezembro de 2015 nº C01-491/2013 no processo nº A40- 118705/2013.

b) neutralidade e passividade do serviço em relação ao conteúdo;

c) a capacidade tecnológica para prevenir ofensas praticadas por terceiros ou detê-las, removendo ou bloqueando o acesso a conteúdo ou documento ilegal, e, em última instância, suspendendo o domínio.

Baseado nessas atividades e na prática judicial, Burova (2017) e Lorenz (2020) sugerem o agrupamento dos intermediários de informações em três categorias, quais sejam:

a) A primeira categoria é constituída pelos que transmitem dados através das redes de telecomunicações, incluindo a Internet, com base em licença apropriada. Ex: operadoras de telecomunicações, no papel de provedores de conexão;

b) A segunda categoria é formada pelos que ofertam serviços para comunicação e publicações de terceiros. Ex: provedor de hospedagem, provedor de aplicação (redes sociais, e-mail, mensageria), administrador de domínio;

c) A terceira categoria é composta pelos que fornecem acesso a materiais de terceiros. Ex: provedor de hospedagem.

Os mecanismos de busca, embora sejam reconhecidos como intermediários de informações, não se enquadram em nenhum dos critérios acima. Lorenz (2020) propõe a criação de uma quarta categoria para recebê-los, pois a atividade desempenhada pelos mesmos inclui a comercialização de metatags de palavras-chave, para promover a publicidade dos proprietários de sites.

Já os provedores de hospedagem podem ser enquadrados no segundo e no terceiro grupo.

O reconhecimento como intermediário de informações, por si só, é insuficiente para determinar a responsabilização por atos de terceiros.

4.4.5 A responsabilidade civil dos intermediários de informações

A regra geral para a responsabilidade civil dos intermediários de informações é delineada pelo parágrafo 1 do artigo 1253.1 do Código Civil (FEDERAÇÃO RUSSA, 2006c). Interpretando-a, depreende-se que se trata da doutrina da responsabilidade civil subjetiva, segundo a qual a culpa é um dos pressupostos, ao lado da prova do dano e do nexo causal. Assim, os intermediários de informações respondem pela violação à propriedade intelectual[112], no ambiente da rede de informação e telecomunicações, pelos fundamentos gerais previstos na lei, se houver culpa, tendo em conta as especificidades estabelecidas nos parágrafos 2 e 3 do referido artigo, que especificam a responsabilidade frente à natureza do serviço prestado.

Para questões sobre violação à propriedade intelectual, os provedores de serviços encarregados pela transmissão de dados são isentos de responsabilidade, caso:

a) não tenham iniciado a transmissão do conteúdo nem designaram o destinatário da informação;

112 O referido artigo protege o direito à propriedade intelectual.

b) não modificaram o conteúdo durante a prestação de serviços, salvo as necessárias ao processo técnico de transmissão;

c) não sabiam, nem tinham condições de saber, a natureza ilícita do conteúdo transmitido.

Para os provedores de acesso, de armazenamento e de aplicação, são isentos de responsabilidade, se:

a) não sabiam, nem deveriam saber, que o uso de objetos de propriedade intelectual era ilegal;

b) após o recebimento de uma notificação do titular de direito lesado, por escrito, indicando a página do site e (ou) o endereço da rede na Internet em que o referido material é publicado, adotaram, imediatamente, as medidas necessárias e suficientes, conforme estabelecido por lei, para cessar a violação ao direito.

Por fim, é importante ressaltar que, mesmo não sendo responsáveis por eventual violação a direito autoral, os intermediários tecnológicos podem ser objeto de medidas cautelares e probatórias, como busca e apreensão no ambiente digital, afastamento do sigilo dos dados, além de cumprir determinação de remoção de conteúdo ilegal ou a restrição de acesso[113].

Quando a violação se refere a pirataria digital de filmes, séries, streaming e outros objetos de direito autoral (exceto fotos), a competência exclusiva para processar e julgar é do Tribunal da cidade de Moscou[114], que pode expedir medidas liminares, atendendo a pleito do titular do direito violado.

Ao *Roskomnadzor* cabe o cumprimento dessas decisões judiciais, além de exercer sua função de órgão fiscalizador, atuando em conformidade com os procedimentos estabelecidos para restringir o acesso a conteúdos infringentes a direitos autorais e (ou) direitos conexos[115]. Em caso de descumprimento, os provedores de serviço estarão sujeitos a bloqueio realizado pelas operadoras de telecomunicações.

113 Parágrafo 4 do Artigo 1253.1 do Código Civil (FEDERAÇÃO RUSSA, 2006c).

114 De acordo com a Lei Federal nº 187-FZ, de 02 de julho de 2013, que alterou o Código Civil, o Código de Processo Civil, o Código de Processo *Arbitrazh* (Comercial) e a Lei nº 149-FZ, 2006 (FEDERAÇÃO RUSSA, 2006a), sobre informação, tecnologias da informação e proteção da informação, fortalecendo a proteção de filmes on-line. Em Novembro de 2014, com a Lei Federal nº 364-FZ (Lei Anti-Pirataria), foi incrementada a lista de objetos de proteção de direitos autorais na Internet (exceto fotos), além de introduzido o banimento perpétuo para sites reincidentes e do processo de notificação e remoção de conteúdo.

115 Nos termos do "Artigo 15.2 Procedimento para restringir o acesso a informações distribuídas em violação de direitos autorais e (ou) direitos conexos", da Lei Federal nº 149-FZ, de 2006 (FEDERAÇÃO RUSSA, 2006a).

5 COMPARATIVOS CONCEITUAIS

O rastreamento do uso e sentidos dos conceitos é, como dito na introdução, o objetivo central de uma metodologia histórico-conceitual. Para explicitar, em nível metodológico, aquilo que acontece na observação direta das fontes primárias, Koselleck (2006) estabeleceu algumas perguntas, não exaustivas, que podem apontar para a relação palavras (significantes) e significados.

É vital lembrar, como feito no primeiro volume deste estudo, que a fonte tem poder de veto (KOSELLECK, 2006, p. 186), ou seja, ao pesquisador(a) é possível revelar o que é de condizente e até o que está subjacente à fonte, mas nunca negá-la, frontalmente.

É pelo comparativo dos conceitos que se revela, por exemplo, os aspectos de "ponto" (sincronia) e "fluxo" (diacronia), além dos diferentes extratos da história e dos recortes gerativos. A demarcação contextual também permite entender até que ponto há uma relação de "globalização", pois as tecnologias em geral pressupõem o aumento constante dessa interação, e até que ponto temos um fechamento e genealogia mais restrita das ideias, ações políticas e conceitos de determinada sociedade.

Após explorar questões analisadas abaixo, adaptadas ao contexto da presente investigação (KOSELLECK, 1967 apud BENTIVOGLIO, 2010, p. 119), foram encontradas as seguintes respostas:

5.1 Que conceitos principais são recorrentes nas tentativas legislativas analisadas?

Na Austrália, para referir à responsabilidade dos provedores, é comum o uso do termo *"strict liability"* (responsabilidade objetiva) ou apenas *"liability"*, bem como *"immunities"*, para aludir aos safe harbors. A legislação também faz referência ao "notice and takedown procedure", processo de notificação de provedores, especialmente diante de violações de normas de direitos autorais.

No BSA, aparecem expressões como *"online content service provider"*, *"platform content"*, *"internet service providers"* (ISPs) e *"internet intermediary"*. Os dois primeiros se referem a provedores que, de alguma forma, disponibilizam conteúdo online, seja criando o próprio material que é disponibilizado *("online content service")* ou fornecendo conteúdo produzido por terceiros *("platform content")*. Já os "internet service providers" (ISPs) se diferenciam destes por não prestar serviços relacionados à produção de conteúdo, não sendo responsáveis, de acordo com a lei, por avaliá-los. Nessa categoria,

enquadram-se os chamados *"application service provider"* (ou seja, aqueles que facilitam o acesso ao conteúdo online, seja indexando, formatando ou filtrando, função normalmente exercida por mecanismos de busca como o Google), os *"host provider"* (definidos como aqueles que hospedam sites, oferecem espaço de armazenamento e conexão à internet) e os *"internet access provider"* (são aqueles que possibilitam a conexão à Internet), sendo todos também considerados *"Internet Intermediaries".*

No *Telecommunications Act*, assim como no *Copyright Act*, é possível identificar a utilização do termo *"carriage service providers"* (CSP) - ou *"Carriage service intermediaries"*-, definidos como aqueles que oferecem serviços de transporte de comunicações ao público, utilizando unidades de rede de propriedade de uma operadora ou através de unidades cobertas por uma declaração. A Subdivisão B do *Copyright Act* descreve, nesse sentido, quatro categorias de atividades desempenhadas pelos *"carriage service providers"* consideradas relevantes para os fins da lei de direitos autorais, que compreendem serviços relacionados à transmissão de informações, cache, hospedagem e mecanismos de busca.

Sob os *Defamation Acts*, os intermediários que tiverem alguma relação, mesmo que mínima com alguma publicação difamatória, podem ser enquadrados no conceito de *"publisher"* (editor) e serem responsabilizados civilmente pela publicação de um conteúdo ofensivo publicado por terceiro, sendo possível que até mecanismos de buscas seja. Além disso, podem ser responsabilizados por propagandas fraudulentas ou enganosas com base nas normas de defesa dos consumidores. No *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act*, há também as expressões como *"content (social media) websites", "hosting service providers", "internet service providers", "content service providers",* referindo-se aos intermediários que devem remover prontamente materiais definidos como "abomináveis".

No *Online Safety Act* é possível encontrar termos como *"social media services", "relevant electronic services", "designated internet services"* se referindo aos provedores. O *"social media services"* se refere a serviços eletrônicos cujo único ou principal objetivo do serviço é permitir a interação social online entre usuários finais ou viabilizam a postagem de conteúdo. O *"relevant electronic services"*, por sua vez, refere-se a todo e qualquer serviço que permite aos usuários finais se comunicarem entre si. Por fim, o *"designated internet services"* engloba serviços que permitem aos usuários finais acessar materiais através de um serviço de transporte pela Internet ou que entregam materiais a pessoas que possuem equipamento adequado para recebê-lo.

No Canadá, por sua vez, alguns conceitos são novos, apesar da evidente origem, como o *"The Notice and Notice Regime"* (Sistema de Aviso e Aviso), introduzido através da Lei de Modernização de Direitos Autorais no país.

Alguns conceitos já utilizados, como *"liability", "safe harbour" e "harmful content", "information content provider"* também são frequentes nas legislações. Na Jurisprudência Giustra v. Twitter Inc, o conceito *"liability"* aparece 9 vezes. O conceito *"broadcaster"* é utilizado na Lei de Direitos Autorais (CANADÁ, 1985) como referência para faz a transmissão do sinal de comunicação (por exemplo, o rádio ou a TV), porém exclui aqueles que fazem "retransmissão" de sinal.

No documento técnico canadense, o conceito *"harmful content"* aparece 30

vezes, significando os cinco tipos penais já previstos pelo código criminal canadense, porém adaptados ao contexto regulatório abordado. Os conceitos "OCSP" (online communication service provider, ou Provedor de Serviços de Comunicação Online) e "OCSs" (Online Communications Services, ou Serviços de Comunicações Online) aparecem respectivamente 118 e 148 vezes no paper técnico.

Na Indonésia, os provedores de Internet são identificados em nomenclatura genérica Operador de Sistemas Eletrônicos (Privados).

Finalmente, na Federação Russa, os principais conceitos legais são apresentados pela Parte Quatro do Código Civil (FEDERAÇÃO RUSSA, 2006c) e pelo Artigo 2 da Lei Federal nº 149-FZ, de 2006, sobre Informação, Tecnologias da Informação e Segurança da Informação (FEDERAÇÃO RUSSA, 2006a).

O Código Civil (Parte Quatro) conceitua intermediários da informação, que abrange entidades que transmitem conteúdos através de uma rede de informações e telecomunicações, inclusive a Internet, ou oferecem recursos para que terceiros o façam ou disponibilizam informações sobre o acesso aos mesmos, além dos que permitem o acesso a conteúdos através de tais tecnologias.

A Lei Federal nº 149-FZ (FEDERAÇÃO RUSSA, 2006a) é mais abrangente, apresentando 18 (dezoito) conceitos legais referentes à ciência da computação, como "informações", "tecnologias da Informação", "tecnologia da informação", "mensagem eletrônica", "site", "Internet", dentre outros.

5.2 Quais conceitos são novos?

Nos últimos anos, as leis que entraram em vigor introduziram novos conceitos ao complexo arcabouço legal da Austrália. O *News Media and Digital Platforms Mandatory Bargaining Code*, por exemplo, traz a expressão digital platforms sem, no entanto, defini-la. A ideia de um conceito aberto é abarcar os vários tipos de plataformas, cabendo ao ministro do *Department of the Treasury* equalizar interesses em questão traçando um conceito. O *Online Safety Act* também insere novos termos como social media services, *relevant electronic services, designated internet services*. No *Social Media (Anti-Trolling) Bill,* também é possível encontrar menções ao *social media services*, já definido pelo *Online Safety Act.*

Além disso, é importante notar que os tribunais também têm um papel importante na criação de novos conceitos, como ocorre no caso de *"publisher"*, que passou a compreender também atividades desempenhadas por alguns tipos de provedores.

Na Legislação canadense, tem-se a inserção do conceito dos "OCSP", *Online "Communication Service Provider"*, em inglês (em português, Provedor de Serviços de Comunicação Online), que se refere aos provedores de aplicação, ou aqueles que provem o serviço de acesso à Internet, em complemento ao que a legislação chama de apenas OCS, ou *"Online Communication Service"* (em português, Serviço de Comunicação Online), também chamados provedores de aplicação (plataformas de conteúdo). É interessante ressaltar que essa diferenciação não é feita no Brasil a partir do Marco Civil da Internet, no qual a categoria mais comum e a diferenciação feita é entre os provedores de conexão

versus os provedores de aplicação.

Na Indonésia, o termo genérico utilizado na legislação para referir os provedores de Internet é "Operador de Sistema Eletrônico". Quando se tratar de instituição privada, utiliza-se o "privado" para distinguir dos provedores de Internet mantidos e administrados pelo Estado, aos quais não se aplicam as leis referidas no presente Relatório.

Na Lei de Informações russa, novos conceitos foram introduzidos, como:
a) "provedor de hospedagem", que presta serviços de fornecimento de poder computacional para postagem de informações em sistema de informação permanentemente conectado à Internet (introduzido pela Lei Federal nº 139-FZ de 28 de julho de 2012);
b) "organizador da divulgação de informações na Internet", que é a pessoa responsável pelo funcionamento de sistemas de informação e/ou aplicativos destinados a receber, transmitir, entregar e (ou) processar mensagens eletrônicas dos usuários da Internet, introduzido na Lei de Informações pela Lei Federal nº 97-FZ, de 05 de maio de 2014.

5.3 Com que outros termos os conceitos listados aparecem relacionados, seja como complemento ou como oposição?

Na Austrália, os tipos de provedores estão normalmente relacionados com as funções que desempenham e com as finalidade para as quais se destinam. Com a preocupação crescente do governo em tornar a Internet um lugar "seguro" e combater o *"serious harm"*, é comum a associação desse termo com a classificação dos conteúdos que devem ser removidos prontamente pelos provedores.

No BSA, por exemplo, é possível encontrar termos como *"Internet content"* associados ao conceito de provedores e às imunidades que estão previstas na lei limitando o seu alcance. Em normas como o *Copyright Act*, UDA e legislação de defesa dos consumidores é possível também encontrar expressões como *"authorise", "publisher"* e *"misleading and deceptive advertisement",* respectivamente. Já em relação ao *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act* 2019, é introduzido o conceito de conteúdos "abomináveis", que abarca todo e qualquer material que registre ou transmita condutas, consideradas ofensivas por pessoas razoáveis, que envolvam terrorismo, assasinato (ou a tentativa), tortura, estupro e sequestro. O *Online Safety Act*, por sua vez, amplia a categoria de conteúdos considerados prejudiciais através dos esquemas regulatórios de *cyberbullying*, imagem íntima divulgada sem consentimento, material abusivo para adultos e conteúdo ilegal e restrito.

Também é possível encontrar o conceito de responsabilidade associado com a noção de *"actual knowledge"* e *"strict"*. Já que, na maioria dos casos, a simples notificação do reclamante é capaz de gerar a responsabilização do intermediário.

No Canadá, os dois conceitos de OCSP e OCS, já mencionados acima, surgem a partir de documento técnico *("Technical Paper")* redigido pelo Governo canadense. Nele,

é expressa a informação de que os OCS seriam as próprias plataformas ou páginas de conteúdo em si, enquanto o OCSP seria o provedor daquela mesma plataforma.

São dois conceitos diferentes para o que na legislação brasileira é chamado apenas de "provedor de aplicação", já que os provedores de conexão não possuem o mesmo significado de "provedor de aplicação" no Brasil. Segundo a legislação brasileira, os provedores de conexão são, na verdade, os que permitem o acesso a Internet, como as operadoras de telefonia móvel; enquanto que os provedores de aplicação operam acima da camada de conexão, tomando como base a própria estrutura técnica da rede *(Facebook, Twitter, Google,* seriam, por exemplo, provedores de aplicação). Segundo a seção Interpretação *("Interpretation")*, no documento técnico canadense:

> 4. *The Act should provide that Online Communication Service Provider (OCSP) means a person who provides an OCS. It should not include a person who provides only a telecommunications service, as those terms are defined in subsection 2(1) of the Telecommunications Act, by reason only that another person uses their telecommunications service or telecommunications facility to provide an OCS. It should not include a person who indicates the existence or location of content or hosts or caches the content or information about the location of the content, by reason only that another person uses their services to provide an OCS.* (CANADÁ, 2022c).[116]

Os OCS estão relacionados às categorias de serviço, enquanto os OCSP, aos serviços em s (o que mais se assemelha aos provedores de aplicação pela legislação brasileira). Além disso, o documento técnico canadense não inclui os serviços de mensageria privada, como o WhatsApp. Segue:

> 2. *The Act should define the term Online Communication Service (OCS) as a service that is accessible to persons in Canada, the primary purpose of which is to enable users of the service to communicate with other users of the service, over the internet. It should exclude services that enable persons to engage only in private communications* (CANADÁ, 2022c).[117]

O documento técnico, que foi um dos documentos mais importantes a motivar o Canadá no amadurecimento para a criação de uma legislação específica voltada a moderação e responsabilidade civil de plataformas, deixa claro que exclui de tais obrigações e sanções previstas no paper os "servidores de conexão" quando diz que a lei estabelece que Provedor de Serviços de Comunicação Online (OCSP) significa uma pessoa que fornece um OCS, não uma pessoa que fornece apenas um serviço de telecomunicações.

---

116 Em português: "A lei deve estabelecer que Provedor de Serviços de Comunicação Online (OCSP) significa uma pessoa que fornece um OCS. Não deve incluir uma pessoa que forneça apenas um serviço de telecomunicações, conforme esses termos são definidos na subseção 2(1) da Lei de Telecomunicações, apenas pelo motivo de outra pessoa usar seu serviço de telecomunicações ou instalação de telecomunicações para fornecer um OCS. Não deve incluir uma pessoa que indique a existência ou localização de conteúdo ou hospede ou armazene em cache o conteúdo ou informações sobre a localização do conteúdo, apenas pelo motivo de outra pessoa usar seus serviços para fornecer um OCS." (CANADÁ, 2022c).

117 Em português: "A Lei deve definir o termo Serviço de Comunicação Online (OCS) como um serviço acessível a pessoas no Canadá, cujo objetivo principal é permitir que os usuários do serviço se comuniquem com outros usuários do serviço pela Internet. Deve excluir serviços que permitem que as pessoas se envolvam apenas em comunicações privadas." (CANADÁ, 2022c).

O documento técnico afirma que não deve incluir nesta categoria uma pessoa que indique a existência ou localização de conteúdo, ou que seja o hospedeiro ou pessoa que armazena em cache o conteúdo ou informações sobre a localização do conteúdo (CANADÁ, 2022c).

Na Indonésia, a terminologia "Operador de Sistemas Eletrônicos" surge relacionada a indivíduos ou instituições, estrangeiros ou domésticos, que operem sistemas eletrônicos para usuários indonésios. Traz o adjetivo privado para distinguir dos mantidos e operados pelo Estado, sobre os quais as normas aqui estudadas não incidem.

Igualmente, refere-se a provedores *Over the Top*, definidos como aqueles que prestam serviços de streaming de vídeo e que funcionam diretamente pela Internet. Segundo Carta Circular nº 3/2016, do Ministro das Comunicações e Tecnologia da Informação esses provedores devem permitir a interceptação de informações para fins de investigação criminal (REPÚBLICA DA INDONÉSIA, 2016), o que coloca em risco a integridade das comunicações no país (FREEDOM HOUSE, 2021).

Na Rússia, "intermediário de informações" é o termo genérico que aparece relacionado a vários tipos de provedores da Internet, como de conexão, de aplicação, de hospedagem, de serviços em nuvem. Alcança também os registradores e administradores de domínio e os mecanismos de busca.

5.4 Qual o espectro social de seu uso? Seu sentido foi objeto de disputa entre setores?

É possível notar que a Austrália, na tentativa de expandir as leis e torná-las mais "fortes" para proteção da segurança no ambiente online, adota uma postura mais incisiva em relação aos provedores. Nesse sentido, percebe-se uma preocupação crescente em tornar mais "eficiente" a detecção e a retirada de conteúdos considerados nocivos.

Para isso, o governo vem ampliando as obrigações dos provedores, sem que haja, no entanto, uma discussão mais aprofundada sobre a questão. Os tribunais também são responsáveis por introduzir mudanças no sistema jurídico australiano, reformulando o alcance de termos já existentes.

Isso tudo, no entanto, é visto com preocupação pela academia, a sociedade civil e por empresas do setor. Já que, além da falta de coerência entre os sistemas legais existentes, as leis aprovadas podem criar um ambiente propício à censura, trazer prejuízos à privacidade e aumentar práticas vigilantistas no país.

No caso do Canadá, as legislações que introduziram os novos conceitos e que resgataram anteriores tiveram (ainda possuem), de certa forma, o objetivo disseminar a produção de conteúdo feito por e em território canadense. Assim, tais conteúdos teriam prioridade nos termos de busca em plataformas de mídia assim como priorização na visualização organizada pelos algoritmos das plataformas.

Porém, a regulamentação de conteúdos exibidos nas plataformas dariam mais poder ao órgão administrativo CRTC – *Canadian Radio-Television and*

Telecommunications Commission. Tanto a Bill C-10 quanto a Bill C-11 receberam críticas dos quatro setores a respeito da liberdade de expressão dos criadores de conteúdo. O contexto da criação das novas legislações surge a partir de uma onda de acontecimentos provocados pela disseminação de discurso de ódio e desinformação na Internet e as já citadas influência do CDA (EUA), a partir da assinatura do Acordo entre o México, Estados Unidos e Canadá (USMCA).

Na Indonésia, a Sociedade Civil e a Academia são veementemente contra as normativas RM nº 5/2020 (REPÚBLICA DA INDONÉSIA, 2020) e RM nº 10/2021 (REPÚBLICA DA INDONÉSIA, 2021), pela flagrante violação aos direitos humanos. Segundo trecho da RM nº 5/2020 (REPÚBLICA DA INDONÉSIA, 2020), por exemplo, para combater a desinformação na Internet, os usuários de redes sociais são obrigados a apresentar documento oficial com foto, o que, para alguns setores, constitui grave violação à privacidade do usuário. Já o Governo e outra parcela da sociedade civil percebem as legislações como forma de assegurar a moralidade e a ordem pública, pois conteúdos desinformativos ou falsos estariam sendo veiculados em ataque às instituições políticas do país.

Na Rússia, ao longo dos últimos 05 (cinco) anos, observa-se intenso movimento do Governo, no sentido de editar normas com vistas a fortalecer a soberania do país sobre o ambiente digital, o que vem causando dificuldade na atuação dos intermediários de informações, especialmente os estrangeiros. Desde o início do conflito bélico com a Ucrânia, a Rússia vem intensificando o rigor das penalidades aplicadas a empresas e indivíduos, com a finalidade de controlar os conteúdos que circulam na Internet. Assim, tanto a empresa quanto os seus altos executivos estão sujeitos a multas exorbitantes. Pessoas físicas, como jornalistas e suas fontes, blogueiros e outras personalidades da rede, e o cidadão comum, estão sujeitos a obrigações, sanções e fiscalização periódica pelo Estado, o que, notadamente, vem contribuindo para perseguição a opositores políticos, críticos do governo e da guerra.

5.5 Até que ponto é comum o uso do conceito "intermediário"?

Na Austrália, é possível encontrar o conceito *"Internet Intermediary"* no *Broadcasting Services Act* como toda entidade que fornece "conteúdo online" ao público, incluindo nesta definição plataformas de conteúdo, provedores de serviços de aplicativos, provedores de hospedagem e provedores de acesso à Internet. Além disso, é possível identificar a utilização do termo "intermediário" em leis como o *Telecommunications Act* 1997 e o *Copyright Act* 1998, os quais fazem referência à expressão *"Carriage service intermediaries".*

No Canadá, o conceito de intermediário aparece em 1985 na Lei de Direitos Autorais como alguém que regularmente provê o espaço ou condições para que a outra parte forneça conteúdo que será desfrutado pelo público. Segue:

> *(2) The following definitions apply in subsection (1). Intermediary. Intermediary means a person or entity who regularly provides space or means for works or other subject-matter to be enjoyed by the public* (CANADÁ, 1985).[118]

Porém, a partir das legislações mais atuais, especificamente o documento técnico canadense, este conceito é substituído por "OCSP", *Online Communication Service Provider* (ou Provedor de Serviços de Comunicação Online) e "OCS", o *Online Communication Service* (ou Serviços de Comunicações Online).

Na Indonésia, não foi identificado o uso do termo "intermediário" para referir a provedores de Internet.

As normativas russas trazem o termo genérico "intermediário de informações".

5.6 Qual o contexto histórico que os conceitos aparecem?

A Austrália possui amplo arcabouço legal, com leis que foram se desenvolvendo de forma independente e com contextos históricos diversos, o que torna o sistema legal confuso e, por vezes, antinômico - normas cujo âmbito de aplicação podem criar situações de confronto direto ou indireto.

Em leis como o *Copyright Act*, os *Defamation Acts e o Racial Discrimination Act*, os tribunais tiveram grande influência. No precedente *University of New South Wales vs Moorhouse* foram estabelecidas as regras para verificar se o provedor "autorizou", de alguma forma, a violação de direitos autorais de terceiros. Recentemente, no caso *Fairfax Media Publications v Voller*, o tribunal expandiu o conceito de *"publisher"* para compreender também administradores de páginas de plataformas. Isso, como se viu, deu origem ao *Social Media (Anti-Trolling) Bill.*

No que se refere ao *Copyright Act,* a lei também foi influenciada por países como Estados Unidos e Coréia do Sul. O Acordo de Livre Comércio Austrália-Estados Unidos de 2004, por exemplo, introduziu alterações na lei australiana para equipará-la ao *Digital Millennium Copyright Act* (DMCA). Já o Acordo de Livre Comércio Austrália-Coreia (KAFTA) em 2014 tornou mais simples a identificação de infratores.

Nos últimos anos, percebe-se uma intensificação da atividade legislativa em relação a temas ligados à remoção de conteúdo e vigilantismo. Em 2015, entrou em vigor o *Enhancing Online Safety for Children Act,* com a finalidade de salvaguardar crianças e adolescentes na Internet, definindo dever dos provedores de remover prontamente materiais considerados danosos para esse grupo. Em 2018, foi a vez do *Access and Assistance Act*, lei muito questionada por introduzir mecanismos que enfraquecem a criptografia no país.

Em 2019, o atentado de Christchurch na Nova Zelândia gerou uma enorme

118 Em português: "As seguintes definições se aplicam na subseção (1). Intermediário. Intermediário é a pessoa ou entidade que regularmente cede espaço ou meios para que obras ou outros objetos sejam apreciados pelo público." (CANADÁ, 1985)

comoção no país e serviu como justificativa para a rápida aprovação do *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act*, lei com conceitos vagos que amplia ainda mais as responsabilidade de provedores na Austrália. Em 2021, diante do crescimento acelerado das plataformas digitais e do embate com empresas de notícias australianas, entrou em vigor o *Treasury Laws Amendment (News Media and Digital Platforms Mandatory Bargaining Code) Act.*

A preocupação crescente com a remoção de material online que o governo considera prejudicial levou a aprovação do *Online Safety Act*, que ampliou significativamente as alterações já introduzidas pelo *Enhancing Online Safety for Children Act.*

O Canadá começou a pensar em criar legislação específica a respeito de responsabilização de intermediários na Internet a partir de uma proeminente influência dos Estados Unidos, que possui uma legislação concreta sobre o assunto desde 1996. A seção 230, do CDA americano, continua a influenciar e a ter efeito no país canadense, visto que o acordo mútuo entre os países Estados Unidos, México e Canadá (USMCA) foi assinado em 2018.

Influências de países da União Europeia também tiveram efeito no Canadá, como a legislação já consolidada da Alemanha, NetzDG, que possui algumas similaridades ao documento técnico *("Technical Paper")* proposto pelo Governo canadense em 2021, como, por exemplo, a referência ao código penal dos dois países.

Na Indonésia, a edição do RM nº 5/2020 (REPÚBLICA DA INDONÉSIA, 2020) coincide com um momento de instabilidade social, caracterizado por aumento da violência e abuso aos direitos humanos. Em Papua Ocidental, região rica em recursos naturais explorados pela Indonésia, por exemplo, protestos separatistas e contra manifestações racistas se intensificaram, em meados de 2019.

Perseguição religiosa, facilitada pela disseminação de mensagens de ódio e desinformações pela Internet, o combate ao crime de blasfêmia, também foram justificativas para o governo implementar normas para facilitar a atuação do Estado na identificação dos envolvidos, mas que tornou vulnerável a privacidade da população e limitou o exercício da liberdade de expressão. Segundo Rodriguez (2021), o governo indonésio usou leis de discurso de ódio, concebidas para proteger minorias e grupos vulneráveis, para silenciar dissidentes e pessoas críticas ao governo.

Ademais, não se pode olvidar a influência religiosa e da cultura local na definição do modelo jurídico posto no país. Apesar de ser composta por uma população majoritariamente muçulmana moderada, a Indonésia ainda é fortemente influenciada por uma parcela que organiza seus pensamentos de acordo com a moralidade, ética e pregões religiosos – parte de um acrônimo conhecido por SARA: *Suku, Agama, Ras e Antar golongan,* em português: "Etnicidade, Religião, Raça e Intergrupo" (KAUR et al, 2018), que se reflete nas legislações, doutrinas e jurisprudências relacionadas à regulação de plataformas no país. A ideologia defendida pelo "SARA" motivou a criação de diversos conteúdos de desinformação direcionados à política, e de certa forma, reforça a autoridade do Estado de bloquear conteúdos que possam vir a causar transtornos sociais, manifestações e reuniões públicas.

A Rússia, ao longo da última década, vem implementando medidas cada vez

mais restritivas sobre a atuação de empresas estrangeiras, inclusive as de tecnologia, em território russo, como forma de estabelecer maior controle do Estado sobre as atividades dessas empresas, fortalecer a soberania digital russa e proteger a segurança das informações na Internet. O contexto de crescente intervenção do governo russo na sociedade e nas tecnologias de informação e comunicação, está atrelado a uma proibição de comportamentos minoritários, como no caso da população LGBTQIA+, na expansão de um projeto de controle, que hoje se consolidou com a Guerra da Ucrânia.

5.7 Por quanto tempo tais conceitos estiveram em uso nos ordenamentos jurídicos?

Na Austrália, o *Telecommunication Act* de 1997 trouxe a definição de "Carriage Service Provider". Em 1999, o *Broadcasting Services Amendment (Online Services) Act* (OSA) inseriu uma limitação geral de responsabilidade *("liability")* para os para os *"Internet service provider"* (ISP) e os *"Internet content host"* (ICH). O Acordo de Livre Comércio Austrália-Estados Unidos (AUSFTA) em 2004 alterou o *Copyright Act* de 1968 para inserir para os imunidades para os *"carriage service providers"* e o regime de *"Takedown Notice"*.

No Canadá, a partir da Lei de Direitos Autorais de 1985, o conceito "intermediário" começou a aparecer na legislação como aquela pessoa que permite que o conteúdo seja veiculado entre o público. O conceito do "sistema de aviso e aviso" e *"liability"* aparecem a partir da Lei de Modernização de Direitos Autorais em 2012. O documento técnico canadense introduz os conceitos de OCSP e OCS a partir de 2021. O conceito de *"harmful content"* é introduzido nas legislações analisadas em 2021 a partir do documento técnico e da jurisprudência de *Giustra vs. Twitter*.

Na Indonésia, "Operador de Sistemas Eletrônicos" é a expressão utilizada para referir os intermediários de tecnologia da informação, constante desde 2008, na Lei de Informações e Transações Eletrônicas.

Na Rússia, até meados de 2006, predominava uma abordagem liberal sobre a Internet, sem que o Estado expressasse interesse em sua regulamentação. Foi apenas neste ano, com a Lei da Informação e a vigência da Parte Quatro do Código Civil (FEDERAÇÃO RUSSA, 2006c), que foram introduzidos conceitos relativos ao assunto.

5.8 Qual é o valor dos conceitos analisados na estrutura da linguagem política e social da época?

Na Austrália, em que pese a falta de uniformidade quanto à questão, o país parece caminhar para um endurecimento das normas relativas ao acesso de dados e à moderação e filtragem de conteúdos na Internet, ampliando as demasiadamente as obrigações dos provedores.

A tentativa de conceituar os termos utilizados nas leis não parece levar mais coerência ao sistema legal do país. Isso porque, como se tratam de normas que se desenvolveram de forma independentes entre si, há conceitos que se chocam e criam "lacunas" na lei, aumentando a insegurança jurídica e os riscos para os intermediários operarem no país.

Além disso, ao acomodar conceitos antigos a situações novas, os tribunais acabam criando analogias que distorcem o sentido original dos termos e a finalidade para os quais foram criados, sem haver um amplo debate com os demais setores da sociedade. A longo prazo, as medidas que vêm sendo adotadas no país podem causar efeitos deletérios para os direitos e liberdades individuais dos cidadãos australianos.

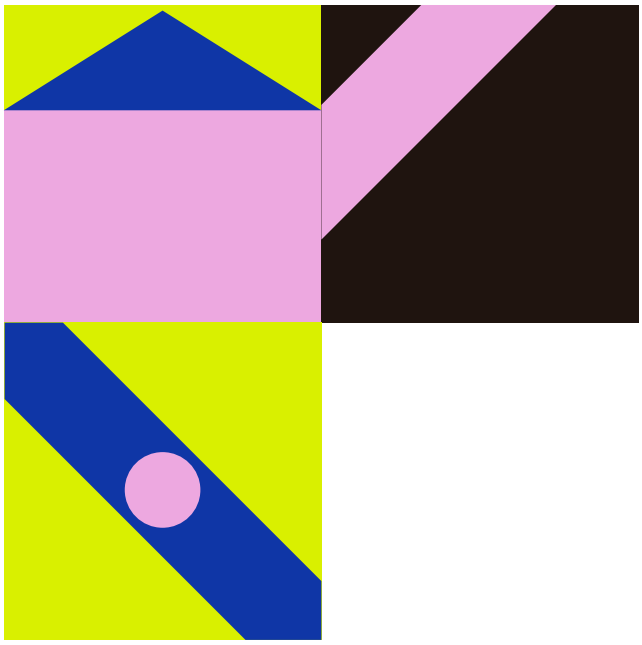
No Canadá, os conflitos entre sociedade civil e governo ainda pesam bastante no que diz respeito a levar adiante as legislações em tramitação para um nível de amadurecimento, aprovação e potencial entrada em vigor. Quando se fala em regulação e responsabilização civil de intermediários, o país parece ter sido influenciado por legislações europeias em vigor, como a alemã NetzDG. No Canadá, assim como vem acontecendo em outros países, a responsabilização penal também vem sendo levantada em muitos aspectos, especialmente quando envolve discurso de ódio, extremismo e terrorismo ou pornografia infantil.

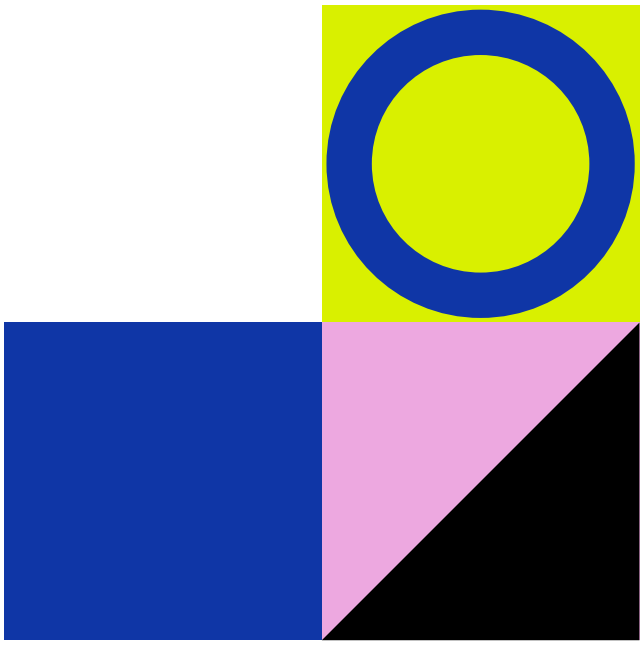
Apesar disso, o país também é fortemente influenciado pela legislação norte-americana, em particular o que é garantido pela seção 230 do CDA pela proximidade geográfica dos países e adesão ao USMCA. No Canadá muito se é discutido, principalmente entre a sociedade civil e a academia, sobre os rumos legislativos de responsabilidade civil no país, e se este tenderá a se aproximar mais dos Estados Unidos (com forte crítica a essa aproximação por parte da academia e sociedade civil), ou de padrões que vêm sendo adotados na União Europeia.

Na Indonésia, os conceitos se apresentam com motivações objetivas e legítimas (combate às *fake news*), mas os instrumentos propostos também servem para regular e cercear a liberdade de expressão, em temas como religião, gênero e orientação sexual. Em certo sentido, portanto, os conceitos são eficientes com o que parece ser o desiderato do Estado: aumento de seu poder e controle geral, através das tecnologias de informação e comunicação. Os dados levantados mostram uma forte tendência ao fechamento de ambiências democráticas e a possibilidade de exercício de direitos.

O ambiente de controle também aparece na Rússia. O país apresenta um conjunto relevante e intrincado - tanto, portanto, no aspecto quantitativo, como qualitativo - de

conceitos que operacionalizam instrumentos jurídicos de controle e redução da esfera de direitos. Há, efetivamente, uma autorização, via lei, para a ampliação da ordem pública. As influências conceituais de outros países europeus, ou do Norte Global, se revelam ambivalentes: mesmos conceitos e sentidos de intermediariedade aparecem para fundamentar controle e criação de obrigações aos provedores (de aplicação e conexão, na terminologia brasileira).





6 COMPARATIVOS ENTRE OS MODELOS

Inovando em relação ao primeiro volume deste estudo, apresenta-se aqui uma análise comparativa entre os modelos de responsabilidade civil de intermediários vigentes nos países pesquisados.

Foram escolhidos os seguintes critérios comparativos: Controle do Estado, Autoridade Administrativa, Controle de Conteúdo e outros temas relevantes ao estudo.

No aspecto relacionado ao "Controle do Estado" (Tabela 3), foram elencados critérios que representam obrigações que devem ser cumpridas pelos intermediários tecnológicos para atuarem no território dos países estudados, que denotam, em sua completude, o nível de influência dos Governos sobre a atuação dos provedores de internet.

Delimitando a abrangência dos requisitos adotados, tem-se que a "Localização de Dados" é a obrigação de manter e processar dados em data centers localizados no território do país onde foram gerados. Para efeito comparativo, considera-se os dados em seu sentido mais amplo, que inclui dados dos usuários, texto de mensagens (e-mails, redes sociais, etc), metadados, e não apenas aqueles que, pela natureza e por força legal, não podem deixar as fronteiras territoriais. Na Austrália e no Brasil, por exemplo, dados de segurança nacional, fiscais e financeiros, dentre outros, devem ser processados e armazenados no território do país. Como critério comparativo, utiliza-se a condição mais ampla, ou seja, que todos os dados e informações originados no país sejam nele processados e armazenados. O Brasil e a Austrália, por exemplo, nesse contexto, não praticam a localização de dados.

A "Representação Local" refere-se à obrigatoriedade de as empresas que operam no país manterem sucursal, representação, filial no território nacional. A "Obrigação de Registro Prévio" concerne ao dever das empresas de se registrarem em determinado órgão estatal antes de iniciarem suas atividades.

Pela análise dos dados compilados na Tabela 3, observa-se que a Rússia, de longe, é o país que apresenta o maior nível de controle sobre as atividades das empresas de tecnologias da informação, em especial as estrangeiras que oferecem serviços aos russos e processam seus dados pessoais.

Apesar de não apresentar um nível de controle tão rígido quanto à Rússia, na Austrália também existem leis que determinam a retenção de dados ou a cópia deles no país. Não há requisitos gerais para a localização de dados pessoais, no entanto em alguns Estados e Territórios exigem um certo nível de retenção e armazenamento de dados para setores específicos, como de saúde e de elegibilidade de crédito (BAKER MCKENZIE, 2023).

O mesmo se percebe na análise da Indonésia, com a exigibilidade de um representante local, o que foi alvo de críticas por outros setores envolvidos na discussão.

Critério\País	Austrália	Canadá	Indonésia	Rússia
Localização de dados	Não	Não	Não	Sim
Representação local	Não	Não	Sim	Sim
Obrigação de registro prévio	Não	Não	Não	Sim

Tabela 3: Controle do Estado

A existência ou não de "Autoridade Administrativa", e suas características, são apresentadas pela Tabela 4. A Rússia, mais uma vez, evidencia seu regime totalitário, mantendo uma autoridade administrativa estatal, o Roskomnadzor (RKN), que atua na regulamentação e fiscalização de diversas áreas (telecomunicações, proteção de dados, direitos autorais, redes sociais, mídia de massa etc), com poderes de determinar a suspensão dos serviços prestados por intermediários de informações, independentemente de decisão judicial.

Na Austrália, o eSafety Commissioner é uma agência instituída para atuar na manutenção da segurança online dos australianos, ao lado da já existente Australian Communications and Media Authority (ACMA). Além de investigar denúncias e desenvolver, junto ao setor, códigos de práticas para regular material considerado prejudicial e registrá-los, atua na proteção dos cidadão australianos por meio da aplicação de esquemas regulatórios (abuso cibernético adulto, *cyberbullying* para crianças, abuso baseado em imagem, conteúdo online ilegal e restrito). Ele também elabora programas de prevenção e de conscientização para a população.

Nos últimos anos, houve um aumento expressivo de seus poderes com a inclusão de outros grupos sociais em seu escopo de proteção. A ampliação desses poderes é, no entanto, alvo de críticas de especialistas da áreas, especialmente no que diz respeito à possibilidade de coleta de informações de suspeitos. Isso porque, apesar de contar com uma equipe multisetorial (educadores, investigadores, advogados, analistas de políticas, especialistas em tecnologias da informação e outros profissionais), não há regras claras que delimitem o exercício desse poder pela agência, o que pode abrir espaço para arbitrariedades (FREEDOM HOUSE, 2022).

No Canadá, foi criado, pelo Governo, o Digital Safety Commissioner, grupo consultivo formado por especialistas em diversas áreas, que atua no combate ao discurso de ódio, a violações a direito autoral, infrações penais na web e outras atividades no ambiente da rede mundial de computadores. Assessora tecnicamente na elaboração de boas práticas e projetos de normas jurídicas voltadas ao combate a essas infrações.

As atribuições de "Autoridade" são albergadas por um Ministério de Estado, na Indonésia. O Kominfo concentra boa parte das competências relativas às obrigações impostas aos intermediários.

Critério\País	Austrália	Canadá	Indonésia	Rússia
Autoridade administrativa	eSafety Commissioner, com o apoio do Australian Communications and Media Authority	Digital Safety Commissioner (proposta em tramitação)	Kominfo	RKN
Natureza	Estatal	Estatal	Estatal	Estatal
Representante sociedade civil	Sim	Sim	Não	Não
Atuação	Restrita	Restrita	Restrita	Ampla

Tabela 4: Autoridade Administrativa

O "Controle de Conteúdo" (Tabela 5) é o terceiro critério comparativo a ser abordado e tem como objetivo principal identificar as principais características concernentes às publicações no ambiente da Internet. No primeiro quesito, o objetivo é identificar se existem normas que autorizam a moderação de conteúdo na web pelo provedor de aplicação ou intermediário de informações.

No enfrentamento à desinformação e à divulgação de notícias falsas, no Canadá, não há previsão legal, embora exista o projeto de lei Bill C-18. A Rússia possui não uma, mas um conjunto de leis. A Austrália, embora não disponha de leis nesse sentido, o ACMA supervisiona o "Código de Prática Australiano sobre Desinformação", desenvolvido voluntariamente pelas empresas do setor.

Quanto à clareza dos conceitos legais que justificam a retirada do conteúdo, a Indonésia utiliza expressões bastante abrangentes, como "ordem pública" e "angústia à comunidade" para referir a conteúdos e documentos proibidos. Na Austrália, há um esforço institucional para definir os termos utilizados. Por essa razão, é possível afirmar que há certa clareza, mesmo que falte uniformidade e coerência em alguns casos e certas normas precisem ser melhor delimitadas.

Acerca de normas específicas sobre responsabilidade civil de intermediários, aos moldes brasileiro, onde o Marco Civil da Internet apresenta a regra geral, é notório que a Austrália e o Canadá disciplinam modelos de responsabilização, mas em legislações específicas, como o *Copyright Act 1968, Broadcasting Act 1992* e mais recentemente o *News Media and Digital Platforms Mandatory Bargaining Code 2021* e o *Online Safety Act 2021.* Além disso, os provedores podem ser responsabilizados com base em leis de proteção dos consumidores, difamação e discriminação racial. No Canadá, está presente na Lei de Direitos Autorais (1985), na Lei de Modernização de Direitos Autorais e na Lei de Modernização das Eleições. Além disso, os provedores podem ser responsabilizados com base no Código Penal, frequentemente sob o tipo penal de "difamação".

Critério\País	Austrália	Canadá	Indonésia	Rússia
Moderação de conteúdo	Sim	Não	Sim	Sim
Legislação de combate à desinformação e fake news	Não	Não	Não	Sim
Definição legal para fake news	Não	Não	Não	Sim
Regime de notificação	Regime de Notificação e Retirada.	Regime de Aviso e aviso	-	-
Retirada de conteúdo (Motivação)	Difamação, propaganda fraudulenta e enganosa, violação de direitos autorais e conteúdos enquadrados nos esquemas de abuso cibernético adulto, cyberbullying para crianças, abuso baseado em imagem, conteúdo online ilegal e restrito.	Difamação e violação a Direitos Autorais	Conteúdos ou documentos que atentam contra a "ordem pública" e os que causam "angústia à comunidade".	Violação a direitos autorais, proteção a crianças, questões militares etc
Clareza dos conceitos legais que justificam a retirada do conteúdo	Sim	Sim	Pouca	Pouca
Normas específicas sobre responsabilidade civil de intermediários	Sim	Sim	Sim	Sim

Tabela 5: Controle de Conteúdo

A tabela 6 apresenta outros quesitos gerais relevantes à análise que não se enquadram nos critérios comparativos acima. O sistema jurídico dos países do Norte Global é o common law; ao passo que, do Sul Global, o civil law.

Considerando o regime político, observa-se que, à medida que o índice de democracia vai aumentando, chegando ao autoritarismo (na Rússia), o modelo de regulação das plataformas apresenta-se severamente restritivo, com forte influência e poder do Estado sobre todas as operações realizadas pelos intermediários de informações, editando leis que favorecem à perseguição a opositores políticos e a

críticos do governo, bem como instrumentalização do Estado com ferramentas jurídicas para interferir na liberdade de informar, de expressar, de opinar.

O sistema jurídico também influencia no modelo vigente. Países onde predomina o Common Law, os precedentes dos tribunais têm grande influência sobre os fatos jurídicos. De acordo com Pappalardo e Suzor (2020, p.476), na Austrália os juízes acabam tendo que realizar um grande esforço interpretativo para criar analogias com expressões que já existem na legislação para resolver os novos casos que surgem *("throw away detail, get rid of particulars").*

Além disso, é possível observar que não existe um direito à liberdade de expressão explícito na Constituição Australiana, que acaba tendo que manipular o conceito aberto de "comunicação política". Outro ponto que chama atenção na Austrália é a questão da remuneração de conteúdo jornalístico, uma vez que o *News Media and Digital Platforms Mandatory Bargaining Code* cria condições para que empresas de notícias negociem com as *Big Techs* o pagamento pelo conteúdo veiculado em suas plataformas digitais.

Critério\País	Austrália	Canadá	Indonésia	Rússia
Remuneração de conteúdo jornalístico	Sim	Não	Não	Não
Natureza	Estatal	Estatal	Estatal	Estatal
Liberdade de expressão na Constituição do país	Não	Sim	Sim	Sim
Sistema jurídico	Common Law	Common Law	Civil law	Civil law
Regime[119] político	Democracia plena	Democracia plena	Democracia fraca	Autoritário
Ranking[120] global	15	12	54	146

Tabela 6: Outros quesitos

---

119 Regime político em 2022, segundo o Índice da Democracia de 2022, elaborado pelo *The Economist Intelligence unit,* uma empresa de pesquisas e análises do *Economist Group,* que publica a revista *The Economist.* O índice analisa cinco fatores diferentes para determinar quais são os países mais democráticos e os mais autoritários do mundo. São eles: características do processo eleitoral e pluralismo, funcionamento do governo, participação política da população, cultura política e liberdades civis. (THE ECONOMIST, 2023).

120 Índice global da democracia, conforme a pesquisa The Economist (2023). A Rússia está na 146ª posição do ranking de 167 países.

CONCLUSÃO

Ao longo da última década, vêm sendo ampliadas as discussões que envolvem o poder e a atuação das grandes empresas de tecnologia da informação, em especial as que veiculam conteúdos na rede mundial de computadores. A depender do regime político do país, a essência das discussões toma feições distintas.

Nos países de democracia plena, como o Canadá e a Austrália, setores da sociedade e representantes do Estado se reúnem em torno do tema, para encontrar a solução ideal, que seja capaz de frear a violência e a mentira praticadas por meio da Internet, sem, contudo, prejudicar o exercício da liberdade de expressão.

Em países onde predomina regime político com viés autoritário, como a Rússia e a Indonésia, iniciativas de regulamentação dos intermediários tecnológicos visam, primeiramente, construir um modelo jurídico que legitime a forte atuação do Estado em defesa de seus interesses, restringindo liberdades e favorecendo a perseguição a opositores políticos, à imprensa livre, a críticos do Governo, estendendo a indivíduos que os retransmitem os produzidos por esses atores. No entanto, como pano de fundo, justificam as medidas com a necessidade de proteção dos seus cidadãos, segurança nacional, combate à criminalidade.

Ocorre que, alguns aspectos restritivos dos modelos da Rússia e Indonésia vêm sendo pensados em países do Norte Global. Na Austrália, por exemplo, a responsabilidade de fiscalizar e aplicar punições é direcionada a órgãos administrativos, que, amiúde, são autorizados a solicitar dados e, inclusive, de pleitear a quebra de criptografia ponta-a-ponta, principalmente quando a infração diz respeito à segurança nacional, discurso de ódio ou extremismo. É importante atentar para que não se torne uma tendência a ampliação da esfera de ordem pública com a diminuição do âmbito dos direitos fundamentais, a partir da legislação. Ademais, há uma tendência dos governos analisados em ampliar as restrições no uso da Internet, aumentando o rol de obrigações dos provedores e criando regime de vigilância e monitoramento.

É inegável, nesse sentido, que a Internet, em sua camada mais próxima do usuário, a de aplicação, tem sido utilizada para facilitar a propagação de conteúdos que incitam a violência, enganam, humilham pessoas, burlam a vontade do povo em processos eleitorais. Por outro lado, em certas ocasiões, é a única ferramenta de que dispõem as vozes dissonantes de um regime opressor, arbitrário e transgressor de direitos humanos. Por essas e tantas outras razões, é importante ampliar o estudo e perseguir um modelo ideal para a responsabilidade civil de intermediários tecnológicos, por danos causados em razão de publicação de seus usuários, cuja fórmula pondere o exercício da liberdade de expressão, a proteção da sociedade contra a violação de direitos humanos, a capacidade tecnológica para intervir e a mínima interferência no modelo de negócio das empresas.

REFERÊNCIAS

ACCESS NOW et al. Indonesia: repeal law that imposes harsh intermediary liabilities, risks curtailing expression. 28 mai. 2021. Disponível em: https://www.accessnow.org/indonesia-intermediary-liabilities. Acesso em: 31 jan. 2023.

ARTICLE 19. Indonésia: Regulations will severely impede internet freedom. Publicado em 04 jul 2022. Disponível em: https://www.article19.org/resources/indonesia-regulations-impede-internet-freedom/. Acesso em: 1 fev. 2023.

AUSTRALASIAN LEGAL INFORMATION INSTITUTE. Telecommunications Act - Sect 87. 1997. Disponível em: http://classic.austlii.edu.au/au/legis/cth/consol_act/ta1997214/s87.html#:~:text=(b)%20a%20network%20unit%20in,is%20 a%20carriage%20service%20provider%20. Acesso em: 10 out. 2022.

AUSTRÁLIA. Telecommunications and Other Legislation Amendment (Assistance and Access) Act. 2018. Disponível em: https://www.legislation.gov.au/Details/C2018A00148. Acesso em: 16 out. 2022.a

AUSTRÁLIA PASSES STRICT INTERMEDIARY LIABILITY LAW. Digital Watch Observatory. 2019. Disponível em: https://dig.watch/updates/australia-passes-strict-intermediary-liability-law. Acesso em: 10 fev. 2023.

AUSTRÁLIA. Australia Attorney-General's Department. [entre 2019 e 2022]. Abhorrent violent material. Disponível em: https://www.ag.gov.au/crime/abhorrent-violent-material#:~:text=Removing%20abhorrent%20violent%20material&text=The%20penalty%20for%20a%20person,)%20and%203%20years'%20imprisonment. Acesso em: 22 nov. 2022.

AUSTRÁLIA. Australian Communications and Media Authority. About Carriers And Carriage Service Providers. 23 fev. 2022. Disponível em: https://www.acma.gov.au/about-carriers-and-carriage-service-providers#:~:text=A%20carriage%20service%20provider%20(CSP,by%20a%20%20 nominated%20%20 carrier%20declaratio. Acesso em: 13 out. 2022. a

AUSTRÁLIA. Australian Communications and Media Authority. Avoid sending spam. 09 jun. 2022. Disponível em: https://www.acma.gov.au/avoid-sending-spam. Acesso em: 13 out. 2022.b

AUSTRÁLIA. Australian Communications and Media Authority. News Media Bargaining Code. 18 mai. 2022. Disponível em: https://www.acma.gov.au/news-media-bargaining-code. Acesso em: 13 out. 2022.c

AUSTRÁLIA. Broadcasting Services Act. 1992. Disponível em: https://www.legislation.gov.au/Details/C2021C00042/Html/Volume_2#_Toc62734656. Acesso em: 29 set. 2022.

AUSTRÁLIA. Copyright Act. 1968. Disponível em: https://www.legislation.gov.au/Details/C2017C00180. Acesso em: 12 ago 2022.

AUSTRÁLIA. Copyright Amendment (Online Infringement) Act. 2015. Disponível em: https://www.legislation.gov.au/Details/C2015A00080. Acesso em: 24 set. 2022.a

AUSTRÁLIA. Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act. 2019. Disponível em: http://www.austlii.edu.au/cgi-bin/viewdoc/au/legis/cth/consol_act/sa200366/s16.html?context=1;query=SPAM%20ACT%202003%20-%20SECT%2016;mask_path=. Acesso em: 17 out. 2022.

AUSTRÁLIA. Department of Communications and the Arts. Reviews of the Enhancing Online Safety Act 2015 and the Online Content Scheme - Discussion paper. 2018. Disponível em: https://www.infrastructure.gov.au/sites/default/files/consultation/pdf/reviews-enhancing-online-safety-act-2015-and-online-content-scheme-discussion-paper-mk4.pdf. Acesso: 10 ago 2022.a

AUSTRÁLIA. Department of Foreign Affairs and Trade. Korea-Australia Free Trade Agreement. 2014. Disponível em: https://www.dfat.gov.au/trade/agreements/in-force/kafta/official-documents/Pages/full-text-of-kafta. Acesso em: 29 set. 2022.

AUSTRÁLIA. Department of Home Affairs. Statement of Principles on Access to Evidence and Encryption. 2018. Disponível em: https://web.archive.org/web/20180925154820/https://www.homeaffairs.gov.au/about/national-security/five-country-ministerial-2018/access-evidence-encryption. Acesso: 26 set. 2022.b

AUSTRÁLIA. Department of Infrastructure, Transport, Regional Development, Communications and the Arts. ACMA Legislated Functions. [20--]. Disponível em: https://www.infrastructure.gov.au/media-technology-communications/media-laws-regulation/acma-legislated-functions. Acesso em: 12 ago 2022.

AUSTRÁLIA. eSafety Commissioner. Learn about the Online Safety Act. [202-]. Disponível em:https://www.esafety.gov.au/whats-on/online-safety-act#:~:text=What%20is%20the%20Online%20Safety,harmful%20behaviour%20and%20

toxic%20content. Acesso: 23 out 2022.a

AUSTRÁLIA. eSafety Commissioner. Who we are. [202-]. Disponível em: https://www.esafety.gov.au/about-us/who-we-are. Acesso: 23 out 2022.b

AUSTRÁLIA. eSafety Commisioner. Abhorrent Violent Conduct Powers. dez. 2021. Disponível em: https://www.esafety.gov.au/sites/default/files/2022-03/Abhorrent%20Violent%20Conduct%20Powers%20Regulatory%20Guidance.pdf. Acesso em: 06 fev. 2022.a

AUSTRÁLIA. eSafety Commisioner. Adult Cyber Abuse Scheme. dez. 2021. Disponível em: https://www.esafety.gov.au/sites/default/files/2022-03/Adult%20Cyber%20Abuse%20Scheme%20Regulatory%20Guidance.pdf. Acesso em: 06 fev. 2022.b

AUSTRÁLIA. eSafety Commisioner. Basic Online Safety Expectations. jul. 2022. Disponível em: https://www.esafety.gov.au/sites/default/files/2022-07/Basic%20Online%20Safety%20Expectations%20regulatory%20guidance.pdf. Acesso em: 06 fev. 2022.d

AUSTRÁLIA. eSafety Commisioner. Cyberbullying Scheme. nov. 2021. Disponível em: https://www.esafety.gov.au/sites/default/files/2022-03/Cyberbullying%20Scheme%20Regulatory%20Guidance_1.pdf. Acesso em: 06 fev. 2022.c

AUSTRÁLIA. eSafety Commisioner. Image-Based Abuse Scheme. nov. 2021. Disponível em: https://www.esafety.gov.au/sites/default/files/2022-03/Image-Based%20Abuse%20Scheme%20Regulatory%20Guidance.pdf. Acesso em: 06 fev. 2022.d

AUSTRÁLIA. eSafety Commisioner. Online Content Scheme. dez. 2021. Disponível em: https://www.esafety.gov.au/sites/default/files/2022-03/Online%20Content%20Scheme%20Regulatory%20Guidance.pdf. Acesso em: 06 fev. 2022.e

AUSTRÁLIA. eSafety Commisioner. Online Safety Act 2021 Sheet. jan. 2022. Disponível em: https://www.esafety.gov.au/sites/default/files/2021-07/Online%20Safety%20Act%20-%20Fact%20sheet.pdf. Acesso em: 06 fev. 2022.e

AUSTRÁLIA. Federal Court of Australia. POKÉMON COMPANY INTERNATIONAL, INC. V REDBUBBLE LTD [2017] FCA 1541. 19 dez. 2017. Disponível em: https://www.judgments.fedcourt.gov.au/judgments/Judgments/fca/single/2017/2017fca1541. Acesso em: 20 out. 2022.a

AUSTRÁLIA. Federal Court of Australia. ROADSHOW FILMS PTY V IINET LTDA [2012] HCA 16; 20 abr. 2012. Disponível em: https://www.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/HCA/2012/16.html?context=1;query=Roadshow%20Films%20Pty%20Ltd%20&%20others%20v%20iiNet%20Ltd;mask_path=. Acesso em: 20 out. 2022.a

AUSTRÁLIA. High Court of Australia. FAIRFAX MEDIA PUBLICATIONS V VOLLER [2021] HCA 27. 20 dez. 2021. Disponível em: https://eresources.hcourt.gov.au/downloadPdf/2021/HCA/27. Acesso em: 25 out. 2022.f

AUSTRÁLIA. High Court of Australia. GOOGLE INC. V AUSTRALIAN COMPETITION AND CONSUMER COMMISSION (2013) 249 CLR 435; [2013] HCA 1. 6 fev. 2013 Disponível em: https://www.judgments.fedcourt.gov.au/judgments/Judgments/fca/single/2017/2017fca1541. Acesso em: 20 out. 2022.

AUSTRÁLIA. High Court of Australia. UNIVERSITY OF NSW V MOORHOUSE [1975] HCA 26; (1975) 133 CLR 1. 01 ago 1975. Disponível em: http://www8.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/HCA/1975/26.html?stem=0&synonyms=0&query=University%20Moorhouse. Acesso em: 20 out. 2022.a

AUSTRÁLIA. Judicial Commission of New South Wales. Proceedings for defamation in NSW. 2012. Disponível em: https://www.judcom.nsw.gov.au/publications/benchbks/civil/defamation.html. Acesso em: 18 ago. 2022.b

AUSTRÁLIA. Office of Parliamentary Counsel. Copyright Regulations. 1969. Disponível em: https://wipolex-res.wipo.int/edocs/lexdocs/laws/en/au/au438en.html. Acesso em: 24 set. 2022.

AUSTRÁLIA. Online Safety Act. 2021. Disponível em: https://www.legislation.gov.au/Details/C2021A00076. Acesso em: 13 set 2022.g

AUSTRÁLIA. Racial Discrimination Act. 1975. Disponível em: https://www.legislation.gov.au/Details/C2016C00089. Acesso em: 24 set. 2022.b

AUSTRÁLIA. Social Media (Anti-Trolling) Bill. 2022. Disponível em: https://www.legislation.gov.au/Details/C2022B00015. Acesso em: 20 out. 2022.f

AUSTRÁLIA. SPAM Act. 2003. Disponível em: https://www.legislation.gov.au/Details/C2016C00614#:~:text=This%20Act%20sets%20up%20a,types%20of%20commercial%20electronic%20messages.&text=Unsolicited%20commercial%20electronic%20messages%20must%20not%20be%20

sent.&text=Commercial%20electronic%20messages%20must%20include%20information%20about%20the%20individual%20or,the%20sending%20of%20the%20message. Acesso em: 13 out. 2022.

AUSTRÁLIA. Supreme Court of South Australia. DUFFY v GOOGLE INC [2015] SASC 170 Judgment of The Honourable Justice Blue. 27 out 2015. Disponível em: http://classic.austlii.edu.au/au/cases/sa/SASC/2015/170.html?query=. Acesso em: 10 out. 2022.c

AUSTRÁLIA. Supreme Court of South Wales. X V TWITTER INC [2017] NSWSC 1300, 28 set. 2017. Disponível em: http://classic.austlii.edu.au/cgi-bin/sinodisp/au/cases/nsw/NSWSC/2017/1300.html?stem=0&synonyms=0&query=X%20x%20Twitter. Acesso em: 20 out. 2022.c

AUSTRÁLIA. Supreme Court of Victoria. TRKULJA V YAHOO! INC LLC & ANOR [2012] VSC 88, 15 mar. 2012. Disponível em: http://classic.austlii.edu.au/au/cases/vic/VSC/2012/88.html. Acesso em: 10 out. 2022.c

AUSTRÁLIA. Treasury Laws Amendment (News Media and Digital Platforms Mandatory Bargaining Code) Act. 2021. Disponível em: https://www.legislation.gov.au/Details/C2021A00021. Acesso em: 10 out. 2022.h

AUSTRÁLIA. US Free Trade Agreement Implementation Act. 2004. Disponível em: http://www.sice.oas.org/TPD/USA_AUS/Negotiations/AUSlaw1202004_e.pdf. Acesso em: 20 out. 2022.

B.C. billionaire Frank Giustra settles lawsuit against Twitter. CBC News, 18 de Janeiro de 2023. Disponível em: https://www.cbc.ca/news/canada/british-columbia/twitter-frank-giustra-lawsuit-pizzagate-court-1.6717814#:~:text=Giustra%20sued%20Twitter%20in%202019. Acesso em: 27 fev. 2023.

BAKER MCKENZIE. Global Data Privacy & Security Handbook. Australia. Data Localization/Residency. 13 jan 2023. Disponível em: https://resourcehub.bakermckenzie.com/en/resources/data-privacy-security/asia-pacific/australia/topics/data-localizationresidency. Acesso em: 02 mar 2023.

BALLESTRIN, Luciana. The Global South as a Political Project. E-International Relations. 03 jul. 2020. ISSN 2053-8626. Disponível em https://www.e-ir.info/2020/07/03/the-global-south-as-a-political-project/?preview=true&_thumbnail_id=85885. Acesso: 18 de julho de 2022.

BANKOVSKIY, Anton; SHURMINA, Irina; ELTOVSKIY, Vladislav; MIKHEEVA, Alisa. Russia adopts law forcing foreign IT companies to "land" in the country. CMS Law-Now Russia. Russia. 16 set. 2021. Disponível em: https://www.cms-lawnow.com/ealerts/2021/07/russia-adopts-law-forcing-foreign-it-companies-to-land-in-the-country. Acesso em: 31 ago 2022.

BARATA, Joan; DAIRBEKOV, Ruslan. Federal Law Nº 31-FZ, On Amending the Article 15.3 of the Federal Law "On Information, Information Technologies, and Information Protection". aka "Fake news Law". Stanford World Intermediary Liability Map. March 18, 2019. Disponível em: https://wilmap.stanford.edu/entries/federal-law-no-31-fz-amending-article-153-federal-law-information-information-technologies. Acesso em: 22 jul 2022.a

BARATA, Joan; DAIRBEKOV, Ruslan. Federal Law Nº 426-FZ, On Amending the Law of the Russian Federation "On the Mass Media" and the Federal Law "On Information, Information Technologies and Protection of Information". Stanford World Intermediary Liability Map. December 2, 2019. Disponível em: https://wilmap.stanford.edu/entries/federal-law-426-fz-amending-law-russian-federation-mass-media-and-federal-law. Acesso em: 14 jul 2022.b

BENTIVOGLIO, Julio. A história conceitual de Reinhart Koselleck. Dimensões: Revista de História da UFES, Vitória, v. 24, p. 114-134, 2010.

BIRNBAUM, Michael. Russian Blogger Law Puts New Restrictions on Internet Freedoms. The Washington Post, 31 de julho de 2014, World. Disponível em: https://www.washingtonpost.com/world/russian-blogger-law-puts-new-restrictions-on-internet-freedoms/2014/07/31/42a05924-a931-459f-acd2-6d08598c375b_story.html. Acesso em: 12 out 2022.

BUROVA, Aleksandra Jur'evna. Yu. Проблемы отнесения субъектов к информационным посредникам и выделения их категорий в российском законодательстве (Problemas de classificação de sujeitos como intermediários de informação e separação de suas categorias na legislação russa). Novo boletim jurídico. 2017. Nº 1 (1). — S. 27-33. Disponível em: https://moluch.ru/th/9/archive/66/2372/. Acesso em: 18 nov 2022.

BUZKO, Roman; AGATEEV, Vasily. The Financial Technology Law Review: Russia. Buzko & Partners. The Law Reviews. 21 de abril de 2022. Disponível em: https://thelawreviews.co.uk/title/the-financial-technology-law-review/russia#footnote-028-backlink. Acesso em: 08 set 2022.

CAIXETA, Marina Bolfarine. O Sul global na política e academia. Observatório Brasil e o Sul. 17 de outubro de 2014. Disponível em: https://www.obs.org.br/cooperacao/662-o-sul-global-na-politica-e-academia. Acesso em: 05 mar 2023.

CANADÁ. Baglow v. Smith. 2011 ONSC 5131 (CanLII). 2011. Disponível em: https://www.canlii.org/en/on/onsc/doc/2011/2011onsc5131/2011onsc5131.html. Acesso em: 27 fev. 2023.

CANADÁ. Carter v. B.C. Federation of Foster Parents Assn. 2005 BCCA 398 (CanLII). 2005. Disponível em: https://www.canlii.org/en/bc/bcca/doc/2005/2005bcca398/2005bcca398.html. Acesso em: 27 fev. 2023.

CANADÁ. Copyright Act. 1985. Disponível em: https://laws-lois.justice.gc.ca/eng/acts/c-42/fulltext.html. Acesso em: 20 agosto de 2022.

CANADÁ. Copyright Modernization Act. 2012. Disponível em: https://laws-lois.justice.gc.ca/eng/annualstatutes/2012_20/fulltext.html. Acesso em: 20 agosto de 2022.

CANADÁ. Elections Modernization Act. 2018. Disponível em: https://laws-lois.justice.gc.ca/eng/annualstatutes/2018_31/page-1.html. Acesso em: 10 de outubro de 2022.

CANADÁ. Giustra v Twitter, Inc., 2021 BCSC 54 (CanLII). 2021. Disponível em: https://www.canlii.org/en/bc/bcsc/doc/2021/2021bcsc54/2021bcsc54.html. Acesso em: 20 agosto 2022.a

CANADÁ. Government Bill (House of Commons) C-11 (44-1) - Third Reading - Online Streaming Act - Parliament of Canada. 2022. Disponível em: https://www.parl.ca/DocumentViewer/en/44-1/bill/C-11/third-reading. Acesso em: 7 set 2022.a

CANADÁ. Lehouillier-Dumas c. Facebook inc., 2021 QCCS 3524 (CanLII). 2021. Disponível em: https://www.canlii.org/fr/qc/qccs/doc/2021/2021qccs3524/2021qccs3524.html. Acesso em: 27 fev. 2023.b

CANADÁ. Notices to Canadian Internet subscribers. 2021. Disponível em: https://ised-isde.canada.ca/site/office-consumer-affairs/en/connected-consumer/notices-canadian-internet-subscribers. Acesso em: 20 agosto 2022.c

CANADÁ. Bill C-10: An Act to amend the Broadcasting Act and to make related and consequential amendments to other Acts. 2021. Disponível em: https://www.parl.ca/DocumentViewer/en/43-2/bill/C-10/third-reading. Acesso em: 20 agosto 2022.d

CANADÁ. Bill C-18: An Act respecting online communications platforms that make news content available to persons in Canada. 2022. Disponível em: https://www.parl.ca/legisinfo/en/bill/44-1/c-18. Acesso em: 01 de Março de 2022.e.

CANADÁ. Quebec Act - Act to establish a legal framework for information technology, CQLR c C-1.1. 2022. Disponível em: https://www.legisquebec.gouv.qc.ca/en/document/cs/c-1.1. Acesso em: 20 de fevereiro de 2023.b

CANADÁ. Techincal Paper, Canadian Heritage. 2022. Disponível em: https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/technical-paper.html. Acesso em: 20 agosto de 2022.c

CANADIAN HERITAGE. Government of Canada announces expert advisory group on online safety. 2022. Disponível em: https://www.canada.ca/en/canadian-heritage/news/2022/03/government-of-canada-announces-expert-advisory-group-on-online-safety0.html. Acesso em: 8 set 2022.

CHELYSHKOV, Sergey; IVANENKO, Vitaly. Overview of the Federal Law No. 236-FZ "On the Activities of Foreign Persons on the Internet Information and Telecommunication Network in the Territory of the Russian Federation". Unicon News and Insights. 20 jul 2021. Disponível em: https://www.unicon.ru/en/insights/publication/Overview_of_the_Federal_Law_No_236_FZ/. Acesso em: 02 set 2022.

COSTA, Agustinus Beo Da; WIDIANTO, Stanley. Indonesian internet blocks amid social unrest lawful, court rules. Reuters, 27 out. 2021. Disponível em: https://www.reuters.com/business/media-telecom/indonesian-internet-blocks-amid-social-unrest-lawful-court-rules-2021-10-27/. Acesso em: 31 Jan 2023.

COUNCIL OF EUROPE. Expert Council on NGO Law. Opinion on the Compatibility with European Standards of Recent and Planned Amendments to the Russian Legislation Affecting NGOs. Prepared by the Expert Council on NGO Law of the Conference of INGOs of the Council of Europe. 19 fev 2021. Disponível em: https://rm.coe.int/expert-council-conf-exp-2021-1-opinion-amendments-to-russian-legislati/1680a17b75. Acesso em: 19 set 2022.

D.A. PROSHINA. The History of the Formation of State Control and Supervision in the Field of Information Technology and Communications. International Journal of Humanities and Natural Sciences, vol. 5-3 (68), 2022. DOI:10.24412/2500-1000-2022-5-3-171-174. Disponível em: https://cyberleninka.ru/article/n/istoriya-stanovleniya-gosudarstvennogo-kontrolya-i-nadzora-v-sfere-informatsionnyh-tehnologiy-i-svyazi. Acesso em: 17 ago 2022.

DCMA.com. Does Canada have a version of the DMCA Takedown? 2022. Disponível em: https://www.dmca.com/FAQ/Does-Canada-have-a-version-of-the-DMCA-Takedown. Acesso em: 10 out 2022.

ESTADOS UNIDOS DA AMÉRICA. USMCA - Agreement between the United States of America, the United Mexican States, and Canada. Text United States Trade Representative. 2020. Disponível em: https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/agreement-between. Acesso em: 20 set 2022.

FEDERAÇÃO RUSSA. Estatuto do Roskomnadzor. Regulamento do Governo da Federação Russa Nº 228, de 16 de Março de 2009, Sobre o Serviço Federal de Supervisão de Comunicações, Tecnologia da Informação e Mídia de Massa. Disponível em: https://eng.rkn.gov.ru/about/. Acesso em: 20 set 2022.

FEDERAÇÃO RUSSA. Lei Federal nº 121-FZ, de 20 de julho de 2012, Sobre alterações a certos atos legislativos da Federação Russa em relação à regulamentação das atividades de organizações não comerciais que atuam como agentes estrangeiros. Disponível em: https://perma.cc/5PKS-F8FH. Acesso em: 12 set 2022.

FEDERAÇÃO RUSSA. Lei Federal Nº 149-FZ, de 27 de julho de 2006, Sobre Informação, Tecnologias da Informação e Segurança da Informação. Adotado pela Duma do Estado em 8 de julho de 2006. Aprovado pelo Conselho da Federação em 14 de julho de 2006. Assinado pelo Presidente da Federação Russa em 27 de julho de 2022. Disponível em: http://www.consultant.ru/document/cons_doc_LAW_61798/. Acesso em: 22 out 2022.a

FEDERAÇÃO RUSSA. Lei Federal Nº 152-FZ, de 27 de julho de 2006, Sobre Dados Pessoais. Adotado pela Duma do Estado em 8 de julho de 2006. Aprovado pelo Conselho da Federação em 14 de julho de 2006. Disponível em: https://54.rkn.gov.ru/protection/acts/p35920/. Acesso em: 18 ago 2022.b

FEDERAÇÃO RUSSA. Lei Federal nº 230-FZ, de 18 de dezembro de 2006. Código Civil da Federação Russa. Parte Quatro. Adotado pela Duma do Estado em 24 de novembro de 2006. Aprovado pelo Conselho da Federação em 8 de dezembro de 2006. Disponível em: http://www.consultant.ru/document/cons_doc_LAW_64629/. Acesso em: 22 out 2022.c

FEDERAÇÃO RUSSA. Lei Federal Nº 236-FZ, de 01 de julho de 2021, Sobre as Atividades de Estrangeiros na Rede de Informação e Telecomunicações da Internet no Território da Federação Russa. Adotado pela Duma do Estado em 17 de junho de 2021. Aprovado pelo Conselho da Federação em 23 de junho de 2021. Disponível em: https://236-fz.rkn.gov.ru/. Acesso em: 26 ago 2022.

FEDERAÇÃO RUSSA. Lei Federal Nº 242-FZ, de 21 de julho de 2014, Sobre Alterações a Certos Atos Legislativos da Federação Russa em Parte do Esclarecimento do Procedimento para Processamento de Dados Pessoais em Redes de Informação e Telecomunicações. Disponível em: https://www.consultant.ru/document/cons_doc_LAW_165838/. Acesso em: 18 ago 2022.a

FEDERAÇÃO RUSSA. Lei Federal Nº 255-FZ, de 14 de julho de 2022, Sobre o controle das atividades de pessoas sob influência estrangeira. Adotado pela Duma do Estado em 29 de junho de 2022. Aprovado pelo Conselho da Federação em 8 de julho de 2022. Assinado pelo Presidente da Federação Russa em 14 de julho de 2022. Disponível em: http://actual.pravo.gov.ru/text.html#pnum=0001202207140018. Acesso em: 05 out 2022. a

FEDERAÇÃO RUSSA. Lei Federal Nº 259-FZ, de 14 de julho de 2022, Sobre alterações ao Código de Ofensas Administrativas da Federação Russa. Adotado pela Duma do Estado em 6 de julho de 2022. Aprovado pelo Conselho da Federação em 8 de julho de 2022. Disponível em: http://www.consultant.ru/document/cons_doc_LAW_421794/. Acesso em: 21 ago 2022.b

FEDERAÇÃO RUSSA. Lei Federal nº 277-FZ, de 14 de julho de 2022, "Sobre alterações a certos atos legislativos da Federação Russa". Adotado pela Duma Estatal em 30 de junho de 2022 Aprovado pelo Conselho da Federação em 8 de julho de 2022. Disponível em: http://www.consultant.ru/document/cons_doc_LAW_421855/. Acesso em: 27 fev 2023.c

FEDERAÇÃO RUSSA. Lei Federal nº 31-FZ, de 4 de março de 2022, "Sobre as alterações ao Código da Federação Russa sobre Ofensas Administrativas". Adotado pela Duma Estatal em 4 de março de 2022. Aprovado pelo Conselho da Federação em 4 de março de 2022. Disponível em: http://actual.pravo.gov.ru/text.html#pnum=0001202203040006. Acesso em: 27 fev 2023.d

FEDERAÇÃO RUSSA. Lei Federal nº 31-FZ, de 18 de março de 2019, Sobre as alterações ao artigo 153 da Lei Federal "Sobre informações, tecnologias da informação e proteção da informação". Adotado pela Duma Estatal em 7 de março de 2022. Aprovado pelo Conselho da Federação em 13 de março de 2022. Disponível em: http://actual.pravo.gov.ru/text.html#pnum=0001201903180031. Acesso em: 28 fev 2023.b

FEDERAÇÃO RUSSA. Lei Federal nº 32-FZ, de 4 de março de 2022, "Sobre as alterações ao Código Penal da Federação Russa e os artigos 31 e 151 do Código de Processo Penal da Federação Russa". Adotado pela Duma Estatal em 4 de março de 2022. Aprovado pelo Conselho da Federação em 4 de março de 2022. Disponível em: http://actual.pravo.gov.ru/text.html#pnum=0001202203040007. Acesso em: 27 fev 2023.e

FEDERAÇÃO RUSSA. Lei Federal nº 426-FZ, de 2 de dezembro de 2019, Sobre alterações à Lei da Federação Russa "Sobre os meios de comunicação de massa e à Lei Federal "Sobre Informação, Tecnologias da Informação e Proteção da Informação". Disponível em: https://perma.cc/AJM9-MW8W. Acesso em: 19 set 2022.a

FEDERAÇÃO RUSSA. Lei Federal nº 443-FZ, de 16 de dezembro de 2019, Sobre as alterações ao Código da Federação Russa sobre Ofensas Administrativas. Adotado pela Duma do Estado em 5 de dezembro de 2019. Aprovado pelo Conselho

da Federação em 11 de dezembro de 2019. Assinada pelo Presidente da Federação Russa em 16 de dezembro de 2019. Disponível em: https://perma.cc/EK5G-AJVT. Acesso em: 02 out 2022.c

FEDERAÇÃO RUSSA. Lei Federal nº 63-FZ, de 13 de junho de 1996, "Código Penal da Federação Russa" (conforme alterações da Lei Federal nº 582-FZ, de 29 de dezembro de 2022). Adotado pela Duma Estatal em 24 de maio de 1996. Aprovado pelo Conselho da Federação em 05 de junho de 1996. Disponível em: http://www.consultant.ru/document/cons_doc_LAW_10699/. Acesso em 17 fev 2023.

FEDERAÇÃO RUSSA. The Constitution of the Russian Federation. Adopted at National Voting on December 12, 1993. The Constitution came into force on the day of its official publication. The text of the Constitution was published in Rossiiskaya Gazeta newspaper as of December 25, 1993. Disponível em: http://www.constitution.ru/en/10003000-01.htm. Acesso em: 09 set 2022.

FEDERAÇÃO RUSSA. Tribunal Constitucional da Federação Russa. Decisão N 10-P, datada de 8 de abril de 2014. No caso de verificação da constitucionalidade das disposições do parágrafo 6º do artigo 2º e do parágrafo 7º do artigo 32 da Lei Federal "Sobre Organizações Sem Fins Lucrativos", partes do sexto do artigo 29 da Lei Federal "Sobre Associações Públicas" e parte 1 do artigo 19.34 do Código de Infrações Administrativas em conexão com reclamações da pessoa autorizada SOBRE DIREITOS HUMANOS NA FEDERAÇÃO RUSSA, FUNDAÇÃO "KOSTROMA CENTER FOR SUPPORT OF PUBLIC INITIATIVES", CITIZENS L.G. Kuzmina, S. M. SMIRENSKY E V.P. Yukechev. Disponível em: https://perma.cc/W87C-VZ6D. Acesso em: 02 out 2022.b

FELIPE, Mathias. Empresas de tecnologia assinam lei na Indonésia. Desinformante. 28 jul. 2022. Disponível em: https://desinformante.com.br/empresas-de-tecnologia-assinam-lei-na-indonesia-que-restringe-conteudo/. Acesso em: 1 fev. 2023.

FONSECA, Lucas Ribeiro de Belmont. O Sul Global e o Desenvolvimento do Conceito da Responsabilidade de Proteger: Cibas e o Caso Líbio. 2016. Disponível em: https://repositorio.ufpb.br/jspui/bitstream/123456789/1664/1/LRBF19072017.pdf. Acesso em: 24 set. 2022.

FREEDOM HOUSE. Freedom on the Net 2021: Indonesia. Key Developments, June 1, 2020 to May 31, 2021. Disponível em: https://freedomhouse.org/country/indonesia/freedom-net/2021. Acesso: 25 jan 2023.

FREEDOM HOUSE. Freedom on the Net 2022: Australia. Key Developments, June 1, 2021 to May 31, 2022. Disponível em: https://freedomhouse.org/country/australia/freedom-net/2022. Acesso: 05 jan 2023.

GALEANO, Eduardo Hughes. Veias abertas da América Latina. Tradução de Sérgio Faraco. Porto Alegre, RS: L & PM, 2020.

GEIST, Michael. Picking Up Where Bill C-10 Left Off: The Canadian Government's Non-Consultation on Online Harms Legislation - Michael Geist. 2021. Disponível em: https://www.michaelgeist.ca/2021/07/onlineharmsnonconsult/. Acesso em: 7 set 2022.

GEVORGYAN, Lina. Regulamentação sobre proteção de Dados na Rússia. Instituto de Referência em Internet e Sociedade. Blog. 24 de julho de 2017. Disponível em: https://irisbh.com.br/regulamentacao-sobre-protecao-de-dados-na-russia/. Acesso em: 18 ago 2022.

GLOBAL NETWORK INITIATIVE. GNI Expresses Concerns About and Calls on Indonesia to Reconsider the "MR5" Regulation. GNI, 11 jun. 2021. Disponível em: https://globalnetworkinitiative.org/mr5-indonesia/. Acesso em: 31 jan. 2023.

GRIFFITHS, James. Australia passes law to stop spread of violent content online after Christchurch massacre. CNN. 04 abr 2019. Disponível em:https://edition.cnn.com/2019/04/04/australia/australia-violent-video-social-media-law-intl/index.html. Acesso: 27 set 2022.

HEER, Christopher; LATOSZEWSKA, Annette; et al. Copyright Infringement Online. Heer Law, 2022. Disponível em: https://www.heerlaw.com/copyright-infringement-online. Acesso em: 8 set 2022.

HOVYADINOV, Sergei. Intermediary Liability in Russia and the Role of Private Business in the Enforcement of State Controls over the Internet. In: FROSIO, Giancarlo. Oxford Handbook of Online Intermediary Liability. Oxford University Press, 2020. Disponível em: https://academic.oup.com/edited-volume/34234. Acesso em: 12 out 2022.

HUGHES, John. Active internet users as percentage of the total population in Australia from 2015 to 2022. Statista. Disponível em: https://www.statista.com/statistics/680142/australia-internet-penetration/#:~:text=The%20share%20of%20the%20Australian,22%20million%20subscribers%20in%202022. Acesso: 08 jan 2022.

JOINT-STATEMENT. Global Coalition of NGOs: Repeal MR5 and its amendment MR10. 04 jul 2022. Assinada por: Access Now; ARTICLE 19; Asia Democracy Network (ADN); Cambodia Center for Human Rights, Electronic Frontier Foundation (EFF), Manushya Foundation, Open Net Korea, Southeast Asia Freedom of Expression Network (SAFEnet), The William Gomes Podcast, UK The Kenya Human Rights Commission. Disponível em: https://www.article19.org/resources/

indonesia-regulations-impede-internet-freedom/. Acesso em: 04 fev 2023.

KAUR, Kanchan; NAIR, Shyam; KWOK, Yenni; KAJIMOTO, Masato; CHUA, Yvonne Tan; LABISTE, Ma. Diosa; SOON, Carol; JO, Hailey; LIN, Lihyun; LE, Trieu Thanh; KRUGER, Anne. Information Disorder in Asia and the Pacific: Overview of Misinformation Ecosystem in Australia, India, Indonesia, Japan, the Philippines, Singapore, South Korea, Taiwan, and Vietnam. Publicado em outubro de 2018. Última atualização em março de 2019. Disponível em: https://ssrn.com/abstract=3134581 ou http://dx.doi.org/10.2139/ssrn.3134581. Acesso em 24 de Fevereiro de 2022.

KHEIR, Moustafa; ALAMEDDINE, Hamza; AFIOUNY, Ehab. Defamatory content online: the responsibility of online intermediaries? A comparative analysis of Australia, The United States, The European Union, and Canada's regulatory responses. Birchgrove Legal. 2020. Disponível em: https://birchgrovelegal.com.au/wp-content/uploads/2020/08/OnlineDefamatoryContent.pdf. Acesso em: 18 ago. 2022.

KIMBERLEY EVANS, ALLENS PATENT & TRADE MARK ATTORNEYS. Intermediary Liability and Takedown Policies in Asia. In: Digital Asia Subcommittee of the Internet Committee. 3 dez. 2021. Disponível em: https://www.inta.org/perspectives/committee-reports/intermediary-liability-and-takedown-policies-in-asia/. Acesso em: 06 fev. 2022.

KOSELLECK, Reinhart. Futuro Passado: Contribuição à semântica dos tempos históricos. Rio de Janeiro: Contraponto: Ed. PUC-Rio, 2006.

KRISHNAMURTHY, Vivek; FJELD, Jessica. CDA 230 Goes North American? Examining the Impacts of the USMCA's Intermediary Liability Provisions in Canada and the United States. 2020. Disponível em SSRN: https://ssrn.com/abstract=3645462 or http://dx.doi.org/10.2139/ssrn.3645462. Acesso em: 06 fev. 2022.

LAIDLAW, Emily. Mapping Current and Emerging Models of Intermediary Liability. Universidade de Calgary. 2019. Disponível em SSRN: https://ssrn.com/abstract=3574727 ou http://dx.doi.org/10.2139/ssrn.3574727. Acesso em: 12 out. 2022.

LEWIS, Sarah Jamie. Press Release: Open Privacy Calls On CRTC To Adopt Manila Principles. Open Privacy Research Society, 2018. Disponível em: https://openprivacy.ca/blog/2018/04/04/open-privacy-calls-on-crtc/. Acesso em: 12 out. 2022.

LORENZ, Dmitry. Информационные посредники (провайдеры) в России и зарубежных странах: природа, сущность и типология (Intermediários de informação (provedores) na Rússia e em países estrangeiros: natureza, essência e tipologia). 15 mai. 2020. Disponível em: https://zakon.ru/publication/igzakon/8215. Acesso em: 23 nov. 2022.

MENDES, Filipe. Apple diz que leis australianas de criptografia colocam todo mundo em risco. Tecstudio. 15 out. 2018. Disponível em:https://www.tecstudio.com.br/apple/apple-diz-que-leis-australianas-de-criptografia-colocam-todo-mundo-em-risco/. Acesso em: 27 set. 2022.

OMOND, Andrew; CHAN, Austin; TONNA-BARTHET, Ceara; HURTON, Constance; HORVATH-FRANCO, David; KIMURA, Genki; NWAYGBALA, Glory; AHMED, Humadha; DORER, Katiana; OROZCO, Luz; LUSTED, Madeleine; HOFMANN, Marlies K.; STENDEL, Robert. Regulation of Digital Media and Intermediaries. Faculty of Law, Oxford University. 2021. Disponível em: https://www.law.ox.ac.uk/sites/default/files/migrated/opbp_report-_regulation_of_digital_media_and_intermediaries.pdf. Acesso em: 20 out. 2022.

PAPPALARDO, Kylie. Duty and control in intermediary copyright liability: An Australian perspective. 2015. Disponível em: https://eprints.qut.edu.au/91474/. Acesso em: 01 fev. 2023.

PAPPALARDO, Kylie; SUZOR, Nicolas (Sydiney Law review). The Liability of Australian Online Intermediaries (2018). In: FROSIO, Giancarlo. Oxford Handbook of Online Intermediary Liability. Oxford University Press. 2020. Disponível em: https://academic.oup.com/edited-volume/34234. Acesso em: 12 out 2022.

PAVLOV, Vitaly. FZ-152 Requirements – Does your Company Need to Comply with them?. Cloud4y: Corporate Cloud Provider. 15 set 2020. Disponível em: https://www.cloud4y.ru/en/blog/fz-152-requirements/. Acesso em: 18 ago 2022.

PINO, Bruno Ayllón. Evolução histórica da Cooperação Sul-Sul (CSS). In: SOUZA, A. Repensando a Cooperação Internacional para o Desenvolvimento. IPEA, 2014.

POPOVA, Arina; ARNAUTOVICH, Andrey. UPDATE: A Guide to Legal Research in Russia. Globalex. Hauser Global Law School Program. New York: New York University School of Law. 2017. Disponível em: https://www.nyulawglobal.org/globalex/Russia_Legal_Research1.html. Acesso em: 28 out 2022.

POTKIN, Fanny; SULAIMAN, Stefanno. EXCLUSIVE Indonesia preparing tough new curbs for online platforms-sources. Reuters, Asia Pacific, March 23, 2022. Disponível em: https://www.reuters.com/world/asia-pacific/exclusive-indonesia-preparing-tough-new-curbs-online-platforms-sources-2022-03-23/. Acesso em: 05 fev 2023.

REPÚBLICA DA INDONÉSIA. A Constituição da República da Indonésia de 1945. Disponível em: https://www.mkri.

id/public/content/infoumum/regulation/pdf/uud45%20eng.pdf. Acesso em: 27 fev 2023.

REPÚBLICA DA INDONÉSIA. Ministro das Comunicações e Tecnologia da Informação. Carta Circular nº 3, de 2016. Quanto à Prestação de Serviços de Aplicativos e/ou Conteúdos pela Internet (Over-The-Top). 31 de março de 2016.

REPÚBLICA DA INDONÉSIA. Regulamento do Ministro de Comunicação e Informática nº 5, de 2020, relativo aos Operadores de Sistemas Eletrônicos Privados. Jakarta, Promulgado em 24 de novembro de 2020. Disponível em: https://jdih.kominfo.go.id/produk_hukum/view/id/759/t/peraturan+menteri+komunikasi+dan+informatika+nomor+5+tahun+2020. Acesso em: 30 jan 2023.

REPÚBLICA DA INDONÉSIA. Regulamento do Ministro de Comunicação e Informática N.º 10, de 2021, relativo a Alterações ao Regulamento do Ministro de Comunicação e Informática N.º 5 de 2020 (MR5). Jakarta, promulgado em 21 de Maio de 2021. Disponível em: https://jdih.kominfo.go.id/produk_hukum/view/id/774/t/peraturan+menteri+komunikasi+dan+informatika+nomor+10+tahun+2021. Acesso em: 1 fev. 2023.

RIBEIRO, Bernardo; BELOTTI, Emily Liene. Medidas de localização de dados: ameaça à globalização digital?. Opinião. Consultor Jurídico. 03 ago 2022. Disponível em: https://www.conjur.com.br/2022-ago-03/ribeiroe-belotti-medidas-localizacao-dados. Acesso em: 18 ago 2022.

RICHTER, Andrei. [RU] Foreign IT giants receive special law. IRIS Merlin. Center for Media, Data and Society, School of Public Policy, Central European University (Budapest). 2021. Disponível em: https://merlin.obs.coe.int/download/9258/pdf. Acesso em: 02 set 2022.

RIMMER, Matthew. Robbery under arms: Copyright law and the Australia-United States Free Trade Agreement. First Monday, v. 11, n. 3, 6 mar. 2006.

RODRIGUES, Gustavo; VIEIRA, Victor. Lei Anticripto na Austrália: uma breve análise da Lei de Acesso e Assistência e seus aspectos mais polêmicos. Institute for Research on Internet & Society (IRIS). 14 dez. 2018. Disponível em: https://irisbh.com.br/en/anti-crypto-bill-in-australia-a-brief-analysis-of-the-access-and-assistance-bill-and-its-most-controversial-aspects/. Acesso: 26 set 22.

RODRIGUEZ, Katitza. Indonesia's Proposed Online Intermediary Regulation May be the Most Repressive Yet. Electronic Frontier Foundation. 16 fev 2021. Disponível em: https://www.eff.org/deeplinks/2021/02/indonesias-proposed-online-intermediary-regulation-may-be-most-repressive-yet. Acesso em: 30 jan 2023.

ROSKOMNADZOR. Em uma reunião do Conselho Público sob Roskomnadzor discutiu as últimas mudanças na legislação sobre dados pessoais. Notícias de Roskomnadzor. 11 de agosto de 2022. Disponível em: https://rkn.gov.ru/news/rsoc/news74448.htm. Acesso em: 18 ago 2022.

ROUDIK, Peter. Russian Federation: Restrictions on Media with Foreign Funding Imposed. 2021. Library of Congress United States. Disponível em: https://www.loc.gov/item/global-legal-monitor/2021-05-14/russian-federation-restrictions-on-media-with-foreign-funding-imposed/. Acesso em: 12 set 2022.

SCHMITZ, Cristin. Online streaming bill adds exemption for user content but concerns remain over regulating "programs". The Lawyer's Daily. 2022. Disponível em: https://www.thelawyersdaily.ca/articles/33399. Acesso em: 8 nov 2022.

SHIEBER, Jonathan. Austrália aprova lei para responsabilizar empresas de mídia social por "material violento repugnante". Tech-Crunch. 04 abr 2019. Disponível em: https://techcrunch.com/2019/04/04/australia-passes-law-to-hold-social-media-companies-responsible-for-abhorrent-violent-material/. Acesso: 25 ago 2022.

SLOAN, Nathan. Litigation and dispute resolution, Updates Implications of the High Court's decision in Fairfax Media Publications Pty Ltd v Voller. Mcleods. Data da Publicação: 28 out. 2021. Disponível em: https://www.mcleods.com.au/news/implications-of-the-high-courts-decision-in-fairfax-media-publications-pty-ltd-v-voller/. Acesso em: 29 out. 2022.

SOLOMUN, Sonja; POLATAIKO, Maryna; HAYES, Helen. Platform Responsibility and Regulation in Canada: Considerations on Transparency, Legislative Clarity, and Design. Harvard Journal of Law & Technology. 2021. Disponível em: https://jolt.law.harvard.edu/digest/platform-responsibility-and-regulation-in-canada-considerations-on-transparency-legislative-clarity-and-design. Acesso em: 27 de fev 2023.

THE CENTER FOR INTERNET AND SOCIETY - STANFORD UNIVERSITY. Australia. Wilmap. [s.d.]. Disponível em: https://wilmap.stanford.edu/country/australia#law. Acesso em: 10 jul. 2023.

THE CENTER FOR INTERNET AND SOCIETY - STANFORD UNIVERSITY. Canadá - Wilmap, 19 de junho de 2017. Disponível em: https://wilmap.stanford.edu/entries/copyright-act-rsc-1985-c-c-42. Acesso em: 20 agosto 2022.

THE ECONOMIST. The Economist Intelligence Unit Limited. Democracy Index. 2022. Frontline democracy and the battle for Ukraine. Fev, 2023. Disponível em: https://www.eiu.com/n/campaigns/democracy-index-2022/. Acesso em: 01

mar 2023.

TOWNSEND, Kelly. Snap federal election cuts Bill C-10 short. Playback. 16 de agosto de 2021. Disponível em: https://playbackonline.ca/2021/08/16/snap-federal-election-cuts-bill-c-10-short/. Acesso em: 27 fev. 2023.

TSAI, Daniel. Online platforms must be made liable for third-party hate content — and it might happen soon. The Star. Opinion. 30 de outubro de 2020. Disponível em: https://www.thestar.com/business/opinion/2020/10/30/online-platforms-must-be-made-liable-for-third-party-hate-content.html. Acesso em: 27 fev. 2023.

WHITMORE, Sarah E., GUEST, Lara, OAKE, Adrienne. Media and communications: Risks of liability emerging for online platforms in Canada. Torys Quartely. 2021. Disponível em: https://www.torys.com/our-latest-thinking/publications/2021/11/risks-of-liability-emerging-for-online-platforms-in-canada. Acesso em: 27 fev. 2023.