UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
Câmpus de Bauru

Priscila Romero Sanches

Regulação e autorregulação de plataformas digitais para a sobrevivência das sociedades democráticas

Bauru - SP
2024

Priscila Romero Sanches

Regulação e autorregulação de plataformas digitais para a sobrevivência das sociedades democráticas

Tese de Doutorado apresentada como parte dos requisitos para obtenção do título de Doutor em Comunicação, junto ao Curso de Pós-Graduação em Comunicação.

Linha de Pesquisa: Gestão e Políticas da Informação e Comunicação Midiática

Orientador: Prof. Dr. Danilo Rothberg

Bauru - SP
2024

S211r

Sanches, Priscila Romero
Regulação e autorregulação de plataformas digitais para a sobrevivência das sociedades democráticas / Priscila Romero Sanches. -- Bauru, 2024
334 p. : il.

Tese (doutorado) - Universidade Estadual Paulista (Unesp), Faculdade de Arquitetura, Artes, Comunicação e Design, Bauru
Orientador: Danilo Rothberg

1. Twitter. 2. Normas Regulatórias. 3. Liberdade de Expressão. 4. Privacidade. 5. Segurança. I. Título.

Sistema de geração automática de fichas catalográficas da Unesp. Biblioteca da Faculdade de Arquitetura, Artes, Comunicação e Design, Bauru. Dados fornecidos pelo autor(a).

Essa ficha não pode ser modificada.

ATA DA DEFESA PÚBLICA DA TESE DE DOUTORADO DE PRISCILA ROMERO SANCHES, DISCENTE DO PROGRAMA DE PÓS-GRADUAÇÃO EM COMUNICAÇÃO, DA FACULDADE DE ARQUITETURA, ARTES, COMUNICAÇÃO E DESIGN - CÂMPUS DE BAURU.

Aos 19 dias do mês de fevereiro do ano de 2024, às 14:00 horas, no(a) Auditório da STPG e meet: https://meet.google.com/gnr-vmvs-vyv, realizou-se a defesa de TESE DE DOUTORADO de PRISCILA ROMERO SANCHES, intitulada **Regulação e autorregulação de plataformas digitais para a sobrevivência das sociedades democráticas**. A Comissão Examinadora foi constituida pelos seguintes membros: Professor Associado DANILO ROTHBERG (Orientador(a) - Participação Presencial) do(a) Departamento de Ciências Humanas / Faculdade de Arquitetura Artes e Comunicação de Bauru, Professor Associado CARLO JOSÉ NAPOLITANO (Participação Presencial) do(a) Departamento de Ciências Humanas da Faculdade de Arquitetura, Artes, Comunicação e Design / Universidade Estadual Paulista, Professora Assistente Doutora ROSEANE ANDRELO (Participação Presencial) do(a) Departamento de Comunicação Social da Faculdade de Arquitetura, Artes, Comunicação e Design / Universidade Estadual Paulista , Professor Doutor MIGUEL LUIZ CONTANI (Participação Virtual) do(a) Departamento de Comunicação / Universidade Estadual de Londrina, Professor Adjunto FERNANDO OLIVEIRA PAULINO (Participação Virtual) do(a) Faculdade de Comunicação / Universidade de Brasilia. Após a exposição pela doutoranda e arguição pelos membros da Comissão Examinadora que participaram do ato, de forma presencial e/ou virtual, a discente recebeu o conceito final: aprovada. Nada mais havendo, foi lavrada a presente ata, que após lida e aprovada, foi assinada pelo(a) Presidente(a) da Comissão Examinadora.

Professor Associado DANILO ROTHBERG

AGRADECIMENTOS

Agradeço primeiramente a Deus pelo dom da vida e a possibilidade de enfrentar as minhas limitações num trabalho como este, que tanto me exigiu mentalmente a longo prazo. Muitas vezes me perguntei o porquê de ter dado início a esta jornada. Quando pensava em desistir, sempre me vinha uma força interior e uma sensação de propósito, em terminar esta investigação.

Meus pais, Loide Emídio Sanches e Paulo Romero Sanches, foram essenciais nesta trajetória, me apoiando e dando suporte emocional nos momentos de dúvidas e desânimo. Compreenderam ainda a minha necessidade de isolamento para o andamento da pesquisa que foi cansativa e consumiu boa parte do meu pouco tempo de finais de semana, quando não estava de plantão na minha atividade como editora de TV ou corrigindo trabalho dos meus alunos de Jornalismo da UEL.

Ficam registrados aqui a minha consideração e agradecimento ao meu orientador, o professor Dr. Danilo Rothberg, que me tratou com respeito, fez as correções necessárias do trabalho e me incentivou a encontrar o meu próprio caminho na execução da pesquisa. Quero ainda expressar o meu apreço pela Unesp, que num momento tão caótico como o da pandemia deu andamento às aulas, encontrando uma forma alternativa para que não perdêssemos tempo.

O doutorado me deu bons amigos que quero deixar marcados. A Nayara Kobori, também doutoranda, foi minha parceira em aulas, no estágio docência e em alguns trabalhos acadêmicos, que estão publicados em Anais de eventos e livros. As professoras Dras. Raquel Cabral e Caroline Kraus Luvizotto foram fundamentais no meu desenvolvimento como pesquisadora. Agradeço ainda aos professores que se dispuseram a estar nesta banca de defesa, para fazerem a avaliação da pesquisa.

Por fim, sou grata aos meus alunos, que me olham como espelho, para desenvolverem suas atividades discentes. Aqui talvez esteja a resposta do porquê eu decidi fazer o doutorado: para ser uma docente melhor. Espero continuar servindo como incentivo para que eles cresçam como jornalistas e pesquisadores. Tenho certeza de que a Comunicação tem muito a ganhar com profissionais empenhados em investigar os fenômenos da atualidade.

RESUMO

As plataformas de mídias sociais são a ágora moderna da sociedade contemporânea. Em desenvolvimento desde os anos 2000, as plataformas de mídias sociais concentram o discurso público, relacionamentos pessoais e comerciais, são as principais fontes de informação e compartilhamento de conteúdo. Esta tese analisa a criação das normas autorregulatórias do Twitter, utilizando um cruzamento temporal com Leis propostas, aprovadas ou apenas discutidas nas casas legislativas de Brasil, Estados Unidos e União Europeia. O objetivo deste estudo é verificar se este movimento de autorregulação das plataformas digitais abarca os desafios das sociedades democráticas, assegurando liberdade de expressão, privacidade e segurança. A investigação passa pela aferição das normas autorregulatórias do Twitter, assim como do arcabouço legal de Brasil, Estados Unidos e União Europeia, a partir de 2006 até 2022. Apontamos transformações e retrocessos do processo regulatório. A pesquisa se apoia numa triangulação metodológica, proposta pela Hermenêutica de Profundidade (HP) de Thompson (2011), que passa pela análise de documentos da plataforma, Leis em tramitação e aprovadas, publicações acadêmicas e falas de pesquisadores e legisladores. Como resultados, identificamos que a criação de normas autorregulatórias foi precedida pela discussão, nos parlamentos, de propostas de regulação. A tendência de autorregulação levou em conta projetos de Leis como referência para elaboração de seus termos de serviço, como se as plataformas estivessem respondendo às iniciativas de regulação.

Palavras-chave: Twitter; Normas Regulatórias; Liberdade de Expressão; Privacidade; Segurança.

ABSTRACT

Social media platforms are the modern agora of contemporary society. In development since the 2000s, social media platforms focus public discourse, personal and business relationships, and are the main sources of information and content sharing. This thesis analyzes the creation of Twitter's self-regulatory standards, using a temporal crossover with laws proposed, approved, or just discussed in the legislative houses of Brazil, the United States, and the European Union. The objective of this study is to verify whether this movement towards self-regulation of digital platforms addresses the challenges of democratic societies, ensuring freedom of expression, privacy, and security. The investigation involves measuring Twitter's self-regulatory standards, as well as the legal framework of Brazil, the United States, and the European Union, from 2006 to 2022. We point out advances and setbacks in the regulatory process. The research is based on methodological triangulation, proposed by Thompson's Depth Hermeneutics (HP) (2011), which involves analyzing platform documents, laws in discussion and approved, academic publications and speeches by researchers and legislators. As results, we identified that the creation of self-regulatory standards was preceded by the discussion, in parliaments, of regulatory proposals. The self-regulation trend considered draft laws as a reference for drafting their terms of service, as if the platforms were answering to regulatory initiatives.

Keywords: *Twitter; Regulatory Rules; Freedom of Expression; Privacy; Security.*

LISTA DE FIGURAS

Figura 1 – Avaliação de transparência das plataformas digitais feita pela RDR 71

Figura 2 – Demonstração sobre o grau de liberdade no uso da internet 80

Figura 3 – Site PiliApp utilizado para fazer comparação de textos 105

LISTA DE QUADROS

Quadro 1 – Empresas mais valiosas do mundo 42

Quadro 2 – Mudanças nas práticas jornalísticas na era digital 50

Quadro 3 – Classificação do trabalho em plataformas 56

Quadro 4 – Princípios para exercício da vigilância estatal 84

Quadro 5 – Proposta de apuração de responsabilidades por conteúdo online 91

Quadro 6 – Pesquisadores e legisladores selecionados para análise de entrevistas no Youtube 98

Quadro 7 – Resumo das alterações nas versões da PP e dos TS do Twitter 128

Quadro 8 – Exemplos de mídias sensíveis publicadas no Twitter 142

Quadro 9 – Conteúdo proibido para monetização no Twitter 152

Quadro 10 – Projetos de Leis de regulação propostos no Brasil de 2006 a 2022 160

Quadro 11 – Leis que regulam plataformas digitais e entraram em vigor no Brasil entre 2006 e 2022 163

Quadro 12 – Termos e definições da LGPD sobre tratamento de dados 170

Quadro 13 – Projetos de Leis de regulação propostos nos EUA de 2006 a 2022 190

Quadro 14 – Leis que regulam plataformas digitais e entraram em vigor nos EUA entre 2006 e 2022 202

Quadro 15 – Instrumentos de regulação propostos na UE 2006 a 2022 247

LISTA DE ABREVIATURAS E SIGLAS

App	Aplicativo
APIs	Interfaces de Aplicações de Programação
AS	Artificial Systems
COPPA	Children’s Online Privacy Protection Act
DEA	Drug Enforcement Agency
DHS	Department of Homeland Security
DNS	Domain Name System
DAA	Digital Advertising Alliance
EUA	Estados Unidos da América
CEO	Chief Executive Officer
CEPD	Comitê Europeu para a Proteção de Dados
FCC	Federal Communication Commission
FCO	Federal Cartel Office
FBI	Federal Bureau Investigation
FDPC	Federal Digital Platform Commission
FMI	Fundo Monetário Internacional
FTC	Federal Trade Commission
GAFAM	Acrônimo que designa Google, Amazon, Facebook, Apple e Microsoft
GCHQ	Government Communication Headquarters
GDPR	General Data Protection Regulation
GNI	Global Network Initiative
IA	Inteligência Artificial
IEEE	Instituto de Engenheiros Eletrônicos e Eletricistas
iOS	Sistema Operacional da APPLE

IPAHRCS Internacional Principles on the Application of Human Rights to Communication Surveillance

IBGE Instituto Brasileiro de Geografia e Estatística

MSN The Microsoft Network

NSA National State of Security

OMC Organização Mundial do Comércio

ONU Organização das Nações Unidas

OCDE Organização para a Cooperação e Desenvolvimento Econômico

RFID Identificação por Radiofrequência

RDR Ranking Digital Rights

SBA Small Business Administration

TICs Tecnologias de Informação e Comunicação

TV Televisão

UNESCO Organização das Nações Unidas para a Educação, a Ciência e a Cultura

UE União Europeia

WSIS World Summit of Information Society

www World Wide Web

Sumário

INTRODUÇÃO 13

1 – CONCEITO, HISTÓRIA E DESAFIOS 19
1.1 Breve histórico da internet 19
1.2 Definição de plataformas 23
1.3 Comunicação em rede 27
1.4 Objeto de regulação das plataformas e desafios 31
2 – O PODER DAS BIG TECHS 37
2.1 Indústria cultural 38
2.2 Capitalismo de plataforma 42
2.3 Economia política da comunicação e redes sociais 46
2.4 Exploração da criação de conteúdo pelos usuários 52
2.5 Segurança e privacidade do usuário 57
3 – BASES DE ESTRUTURAÇÃO PARA A REGULAÇÃO DAS PLATAFORMAS 61
3.1 Princípios para a regulação 62
3.2 Regulação, autorregulação e corregulação, diferenças e semelhanças 66
3.3 Transparência na coleta e utilização de dados por parte das plataformas 70
3.4 Transparência na coleta e utilização de dados por serviços público e por parte dos governos 76
3.5 Iniciativas provenientes da sociedade para fiscalização da atuação dos governos e das plataformas de mídias sociais sobre liberdades individuais 83
3.6 Parâmetros normativos legais e de autorregulação das plataformas para identificação e exclusão de conteúdos de desinformação, conteúdo ilegal e discursos de ódio 88
4 – METODOLOGIA 93
4.1 Instrumento de análise documental 94
4.2 Instrumento de revisão sistemática da literatura 95
4.3 Instrumento audiovisual de interpretação de estudiosos e legisladores 97

ANÁLISE DE DADOS 103

5 – NORMAS AUTORREGULATÓRIAS E LEGAIS 103
5.1 Normas autorregulatórias do Twitter 104
5.1.1 Política de Privacidade (PP) 106
5.1.2 Termos de Serviço 117
5.1.3 Documentos avulsos de autorregulação do Twitter 135
5.1.3.1 Normas referentes a conteúdo violento 137
5.1.3.2 Normas referentes a conteúdo inseguro ou ilegal 144
5.1.3.3 Normas referentes a conteúdo relacionado à privacidade do usuário 149
5.1.4 Normas para monetização de conteúdo 151
5.2 Síntese de resultados sobre normas autorregulatórias do Twitter 155
5.3 Análise de mecanismos legais de regulação no Brasil, EUA e União Europeia 159
5.3.1 Mecanismos legais do Brasil 160
5.3.1.1 Lei Carolina Dieckmann (Lei nº 12.737, 2012) 164
5.3.1.2 Marco Civil da Internet (Lei nº 12.965, 2014) 165
5.3.1.3 Minirreforma da Lei Eleitoral (Lei nº 13.488, 2017) 168

5.3.1.4 Lei Geral de Proteção de Dados - LGPD (Lei nº 13.7096, 2018) 168
5.3.1.4 Emenda Constitucional 115/22 174
5.3.1.5 Projetos de Lei referentes à liberdade de expressão 175
5.3.1.6 Projetos de Lei referentes à liberdade de expressão e segurança 177
5.3.1.7 Projetos de Lei referentes à privacidade 178
5.3.1.8 Projetos de Lei referentes à privacidade e segurança 178
5.3.1.9 Projetos de Lei referentes à segurança 179
5.3.1.10 Projetos de Lei referentes à liberdade de expressão, privacidade e segurança 182
5.3.2 MECANISMOS LEGAIS DOS EUA 190
5.3.2.1 Broadband Data Improvement Act - Public Law Nº 110-385, 2008 203
5.3.2.2 Providing Resources, Officers, and Technology to Eradicate Cyber Threats to Our Children Act - PROTECT Our Children Act - Public Law Nº 110-401, 2008 204
5.3.2.3 Children's Online Privacy Protection Act – COPPA Rule, 2013 206
5.3.2.4 Allow States and Victims to Fight Online Sex Trafficking Act – SESTA /FOSTA – Law 115–164, 2018 208
5.3.2.5 Projetos de Lei referentes à liberdade de expressão 210
5.3.2.6 Projetos de Lei referentes à liberdade de expressão e segurança 218
5.3.2.7 Projetos de Lei referentes à privacidade 221
5.3.2.8 Projetos de Lei referentes à privacidade e segurança 228
5.3.2.9 Projetos de Lei referentes à segurança 232
5.3.2.10 Projetos de Lei referentes à liberdade de expressão, privacidade e segurança 244
5.3.3 MECANISMOS LEGAIS DA UNIÃO EUROPEIA 246
5.3.3.1 Diretiva 2010/13UE, atualizada pela Diretiva 2018/1808/UE – Diretiva de Serviços de Comunicação Social Audiovisual 248
5.3.3.2 Diretiva 2011/92/EU 251
5.3.3.3 Regulamento (UE) 2016/679 – Regulamento Geral de Proteção de Dados (RGPD) 253
5.3.3.4 Diretiva 2017/541 e Regulamento (UE) 2021/784 258
5.3.3.5 Diretiva 2019/790 261
5.3.3.5 Regulamento (UE) 2019/1150 262
5.3.3.6 Regulamento (UE) 2022/991 264
5.3.3.7 Regulamento (UE) 2022/1925 – Regulamento dos Mercados Digitais 265
5.3.3.8 Regulamento (UE) 2022/2065 – Regulamento dos Serviços Digitais 267
5.3.3.9 Diretiva (UE) 2022/2555 269
5.4 SÍNTESE DE RESULTADOS DE NORMAS REGULATÓRIAS DE BRASIL, ESTADOS UNIDOS E UNIÃO EUROPEIA 271
5.5 DISCUSSÃO E CRUZAMENTO DE NORMAS AUTORREGULATÓRIAS COM INSTRUMENTOS LEGAIS 276
CONCLUSÃO **296**

REFERÊNCIAS **300**

INTRODUÇÃO

A rede mundial de computadores tem sido objeto de estudos desde a sua concepção. As pesquisas abrangem as mais diversas áreas, desde os avanços tecnológicos alcançados com a evolução digital às mudanças socioeconômicas, proporcionadas por novas formas de trabalho e sustento, assim como políticas, que garantiram maior participação popular e comunicacional, com ampliação das formas de interação e compartilhamento de informações. Relações comerciais e pessoais vêm migrando para o ciberespaço, que tende a concentrar a maior parte da vida cotidiana dos cidadãos. De acordo com a Internacional Telecommunication Union (ITU, 2022), agência da Organização das Nações Unidas (ONU), para mais de 5,3 bilhões de pessoas, que representam cerca de 66% da população mundial, existir na sociedade contemporânea passa pelo acesso à internet.

Desde que a internet foi disponibilizada para uso doméstico, na década de 1990, até a contemporaneidade muita coisa mudou. O discurso público migrou, em grande parte, para as plataformas de mídias sociais. Em ambientes democráticos, há uma busca pela manutenção de um ciberespaço igualitário, que respeite a liberdade de expressão, preservando ainda a privacidade do usuário e sua segurança, na utilização dos serviços online. Na tentativa de estabelecer parâmetros de utilização desta ferramenta, indispensável na atualidade, as sociedades democráticas trabalham na criação de arcabouços legais que atendam ao desafio presente.

O processo de estabelecimento de regras de utilização das plataformas digitais se deu desde quando foram criadas, principalmente por via autorregulatória. O tema é sensível, e é tênue a linha na busca pelo ponto de equilíbrio para evitar a censura do discurso público e prevenir avanços de governos ou do setor privado sobre liberdades individuais, como o direito de livre expressão do pensamento, privacidade e segurança.

O objetivo geral desta pesquisa é identificar se os regramentos criados para utilização das plataformas digitais podem assegurar direitos fundamentais dos cidadãos referentes à liberdade de expressão, privacidade e segurança. Esta tese tem como objetivos específicos: 1) caracterizar as iniciativas de autorregulação do Twitter, desde sua criação em 2006 até 2022; 2) investigar projetos de Leis e instrumentos legais de regulação das plataformas de mídias sociais pelos legisladores de Brasil, Estados Unidos e União Europeia desde 2006 até 2022; 3) identificar no processo

evolutivo das normas autorregulatórias como as propostas legislativas influenciaram a transformação das regras de utilização dos serviços do Twitter; 4) identificar e interpretar transformações e retrocessos na manutenção de um ambiente nacional e global de afirmação do direito à informação e à comunicação, diante das exigências democráticas de responsabilização das plataformas de mídias sociais; 5) indicar as realizações mais bem-sucedidas de equacionamento dos desafios de regulação das plataformas de mídias sociais, oriundas de Leis e instrumentos legais em vigência ou já superados.

Esta tese utiliza como objeto de análise normas regulatórias de Brasil, Estados Unidos e União Europeia e normas autorregulatórias do Twitter, de 2006 a 2022. Foram examinados documentos referentes às normas autorregulatórias, às Leis em discussão e aprovadas, além de estudos publicados que contemplam o tema. Como ação adicional, analisamos falas públicas de pesquisadores e políticos com suas avaliações sobre a regulação das plataformas de mídias sociais. A base metodológica está centrada na Hermenêutica de Profundidade (HP), de Thompson (2011), que propõe uma interpretação dos fenômenos sociais e comunicacionais. Thompson (2011) propõe três etapas analíticas: 1ª) Análise Sócio-histórica, que observa o contexto em que o texto foi criado; 2ª) Análise Formal ou Discursiva, com a interpretação do conteúdo do texto; e, por fim a 3ª) Interpretação e Reinterpretação, que analisa como formas simbólicas foram interpretadas anteriormente.

As normas autorregulatórias e regulatórias foram analisadas a partir dos próprios documentos legislativos e normativos apresentados, com apoio de revisão bibliográfica, falas de estudiosos e legisladores sobre os instrumentos aprovados numa comparação temporal, ano a ano, da apresentação e implantação das regras. Esta tese sustenta que as normas autorregulatórias são impulsionadas pelo movimento regulatório legislativo. Neste sentido, as plataformas digitais são estimuladas à criação de normas autorregulatórias já a partir da discussão dos projetos de Leis nas casas legislativas, utilizando o tema apresentado pelos legisladores para desenvolver regras próprias, antes mesmo que a proposta seja aprovada e sancionada como norma legal.

Esta tese fez o cruzamento ano a ano dos projetos de Leis propostos nas casas legislativas de Brasil, Estados Unidos e União Europeia, com as normas autorregulatórias do Twitter em busca de aproximação temática. Em 2012, por exemplo, quando a plataforma criou a ferramenta Do-Not-Track que poderia ser

acionada quando o usuário não quisesse que seus dados fossem coletados, a norma tinha clara referência a um projeto de lei apresentado no Senado estadunidense no ano de 2011. A ferramenta criada na norma autorregulatória do Twitter fazia exatamente o que propunha o projeto de Lei Do-Not-Track Online Act (S. 913), dando uma oportunidade ao usuário, de negar à plataforma a coleta de seus dados.

Esta tendência, de que o movimento autorregulatório sucede a ação legislativa, foi notada na correspondência entre temas mais discutidos nas casas legislativas e instrumentos autorregulatórios, fundamentando a inferência de que o ponto de partida de normas do Twitter tenha sido a proposição anterior de projetos de leis pelos parlamentares. Não foi possível verificar, porém, se as normas autorregulatórias se tornaram efetivas, já que fazê-lo extrapolaria as possibilidades metodológicas desta tese.

Foram analisadas 78 normas de autorregulação formuladas pelo Twitter. Estas normas são divididas em moderação de conteúdo, que interferem na liberdade de expressão; regras de tratamento de dados, que influenciam na privacidade; e, normativas sobre cometimento de ilícitos, que impactam a segurança do usuário. Quanto ao quadro regulatório de Brasil, Estados Unidos e União Europeia foram analisados 143 instrumentos legais entre Leis, projetos de Leis, Regulamentos e Directivas. O recorte temporal da amostra é aberto pela data de criação do Twitter, no ano de 2006, e, encerrado pelo fechamento do estudo, antes da venda e mudança de domínio da plataforma de mídia social, em 2022. No ano seguinte, Elon Musk comprou o Twitter e mudou o nome da plataforma para X.

A etapa teórica tem início com o capítulo 1, que traz um breve referencial histórico da internet, com aprofundamento na conceituação de termos, como o que se entende por plataforma digital e de quais têm sido os principais campos de pesquisa desta área. Além disso, foram demonstradas as principais transformações comunicacionais proporcionadas pela rede mundial de computadores e elencados os maiores desafios à regulação das plataformas de mídias sociais, levando-se em consideração a necessidade de manutenção da liberdade de expressão, privacidade e segurança do usuário, que são pontos chaves para as sociedades democráticas.

O capítulo 2 trata da ascensão das empresas de tecnologia no campo econômico. Este avanço tem proporcionado às grandes corporações do setor o domínio de atividades da comunicação, valendo-se de produções de terceiros, sem a devida remuneração dos produtores de conteúdo, e, ainda, expondo estes

profissionais a riscos de responsabilização solidária por mensagens propagadas na rede mundial de computadores, mesmo quando os *posts* são editados ou modificados pelas plataformas para obtenção de melhores resultados de distribuição do material. Por fim, o método de comercialização das plataformas digitais utiliza meios questionáveis para fazer direcionamento de ofertas relacionadas a serviços e produtos, invadindo a privacidade dos usuários e compartilhando seus dados com terceiros sem autorização expressa para esta finalidade.

No capítulo 3 os esforços são concentrados na apresentação dos princípios para a regulação das plataformas digitais. É tratada ainda a conceituação sobre regulação, autorregulação e corregulação. O capítulo trata também da transparência, já que as plataformas não são necessariamente as proprietárias dos dados que coletam, tratam e armazenam. Sendo assim, os donos dos dados, usuários das plataformas, precisam ter acesso às suas informações, assim como compreender como estão sendo utilizadas e compartilhadas com terceiros. A sociedade exerce um papel fundamental de fiscalização do respeito às liberdades individuais dos cidadãos. Em última instância, são apresentados os parâmetros para a responsabilização na emissão de informação nas plataformas de mídias sociais, referente principalmente a conteúdo ilegal, de desinformação ou que incorre em crimes ligados à honra como injúria, calúnia e difamação.

A metodologia de coleta e análise dos dados está descrita no capítulo 4, no qual é detalhado o processo de desenvolvimento da pesquisa. Foram coletados documentos do início das ações de autorregulação, em 2006, até o final de 2022. A seleção do Twitter se deu por ser considerada esta uma rede social que concentra boa parte da discussão pública contemporânea e pela plataforma disponibilizar os arquivos das normas de privacidade e termos de serviço desde a sua criação até a época da coleta de dados, sendo possível resgatar versões anteriores dos documentos. O motor de buscas do Google auxiliou no estabelecimento de data da primeira vez que determinada regra de utilização foi publicada pelo Twitter, tornando possível a inferência de relação entre a apresentação da proposta legislativa com a redação da norma autorregulatória. Os projetos de Leis e legislações em vigor foram coletados dos bancos de informações das casas legislativas de Brasil, EUA e UE.

O capítulo 5 apresenta a análise das normas autorregulatórias do Twitter e as normas regulatórias dos países e bloco econômico selecionados. Inicialmente a análise é feita separadamente, com início pelas normas autorregulatórias abrangendo

documentos, revisão da literatura e falas públicas de pesquisadores sobre este tema. Na segunda parte são analisadas as propostas legislativas de Brasil, Estados Unidos da América e União Europeia sobre a regulação das plataformas digitais utilizando a mesma sistemática das normas autorregulatórias.

Nesta etapa, pela proposta metodológica da HP, são analisados os documentos que representam a estrutura articulada das normas. A revisão da literatura observa as intencionalidades, convenções de produção, circulação e oferecem interpretações das normas como considerações sobre evoluções e retrocessos dos temas. Já nas falas públicas de pesquisadores e legisladores é possível analisar o contexto sócio-histórico em que as normas estão inseridas, e intencionalidades podem ser verificadas nas falas dos estudiosos em suas próprias interpretações.

Ao final do capítulo 5 é feito um cruzamento de informações, demonstrando o que está proposto na tese, de que o movimento autorregulatório é precedido pelo processo regulatório do legislativo. Foi possível observar ano a ano como as normas autorregulatórias ganharam complexidade e se distribuíram dentro da plataforma, no intuito de abarcar as demandas legislativas impostas no decorrer de 16 anos de análise. Depreende-se da pesquisa que, quanto maior for a pressão legislativa, maior tende a ser a resposta autorregulatória das plataformas digitais.

Transformações podem ser notadas nas normativas dos temas propostos: liberdade de expressão, privacidade e segurança. Percebe-se pelo estudo que a temática da privacidade do usuário foi a mais discutida e estruturada até o momento. Foram discutidas e aprovadas Leis de controle sobre o uso dos dados como Regulamento Geral de Processamento de Dados europeu, a Lei Geral de Proteção de Dados brasileira e o assunto segue em discussão nos Estados Unidos. Nota-se uma preocupação com a segurança das crianças contra abuso sexual, visualizada na Allow States na Victims to Fight Online Sex Trafficking (2018) ou Children´s Online Privacy Protection (2013), Leis aprovadas nos EUA.

Um tema bastante discutido, que teve muitas transformações, mas ainda demanda atenção é o da liberdade de expressão, que inclui a moderação de conteúdo. Transformações têm sido feitas como a Diretiva 2017/541, que tratou de conteúdo terrorista na União Europeia. A norma obrigou as plataformas a terem um processo rápido de exclusão de conteúdo de glorificação da violência, em apoio a atos extremistas e contrários a minorias. Mas a análise vai demonstrar que o tema carece

de discussão, por conta das demandas que se multiplicam ano a ano. Até 2022, 25 propostas de Leis nos EUA e oito no Brasil trataram exclusivamente sobre a moderação de conteúdo, porém, sem que os projetos avançassem para aprovação e sanção.

1 – CONCEITO, HISTÓRIA E DESAFIOS

Neste capítulo 1, a tese traz um breve histórico da internet, indicando como ela é examinada em diferentes áreas de estudo. O capítulo abrange a plataformização e a evolução conceitual desde que os sites estáticos, com pouca oferta de interação com o usuário, foram se transformando em infraestrutura tecnológicas multifacetadas, que abrigam inúmeras formas de atividades. A comunicação em rede é discutida sob o aspecto da migração dos relacionamentos humanos do ambiente físico para o virtual em todos os segmentos da vida cotidiana, desde as relações de trabalho até as sociais.

Como último ponto desta etapa inicial da tese, são apresentados os desafios na identificação do objeto de regulação e aplicação das normas regulatórias. Entre as principais dificuldades, estão o fato de que as plataformas digitais são propriedade de empresas transnacionais, para as quais não há uma base legal já constituída em países onde atuam, e, ainda, a constante evolução tecnológica, que torna mais complexa a tarefa de criação de normas atualizadas pelos legisladores locais.

Em conformidade com a proposta desta tese, o capítulo 1 foi dividido em quatro seções. A seção 1.1 discorre sobre a história da internet e a evolução tecnológica da rede mundial de computadores. Na seção 1.2, o conceito de plataformização é trabalhado, com a apresentação das infraestruturas tecnológicas que foram ampliando o espectro de atuação das plataformas na nossa sociedade. A comunicação em rede é tratada na seção 1.3, com a discussão da mudança paradigmática da verticalidade para a horizontalidade na emissão e recepção da informação. A seção 1.4 trata da definição de um dos objetos da regulação nas plataformas digitais, proposto para esta tese, que é a moderação de conteúdo e os principais desafios impostos a esta tarefa.

Como resultado deste capítulo 1, indica-se que as plataformas digitais se valeram de paradigmas do início dos anos 2000 para justificar a falta de normas regulatórias que balizem suas ações. São apresentadas ainda contribuições positivas, como da União Europeia, que tem encontrado maneiras de demarcar regras possíveis para a regulação, na moderação de conteúdo, na busca por ambientes democráticos e seguros aos usuários da rede.

1.1 Breve histórico da internet

A história oficial sobre a criação da internet refere-se a ela como originalmente projetada para fins militares. Entre os anos 1968-69, com financiamento da Administração dos Projetos de Pesquisa Avançada do Departamento de Defesa dos Estados Unidos, a Arpa, foi criada a primeira rede de computadores interligados em rede. Batizada de Arpanet a rede interligava universidades estadunidenses. Seria uma resposta militar ao lançamento do foguete Sputnik da União Soviética, durante a Guerra Fria. O objetivo principal era de que a comunicação fosse mantida, mesmo com a retirada de qualquer máquina da rede, ou mesmo a destruição nuclear da infraestrutura que a mantinha. Em 1975, já havia cerca de dois mil usuários conectados. A visão do Pentágono era de defesa, mas professores e pesquisadores buscavam acesso livre à informação (Briggs; Burke, 2016).

Diferentemente do sistema telefônico, a arquitetura da internet previa a entrega de informações em pacotes, com conexão à rede de qualquer parte do planeta, era esta a grande diferença da nova infraestrutura de comunicação. “O sistema de envio quebrava a informação em peças codificadas, e o sistema receptor juntava-a novamente, depois de ter viajado até seu destino. Esse foi o primeiro sistema de dados empacotados da história” (Briggs; Burke, 2016, p. 301). Em 1986, o mercado introduz o que seria necessário para a utilização comercial da internet, as terminações “.com”, “.mil” para militar e “e” para educação.

Porém, a utilização comercial da internet só foi difundida mesmo a partir da década de 1990, com investimentos massivos do grupo Time/Warner, estadunidense, American On-line, financiados por grupos franceses e alemães e ainda Prodigy. O centro de pesquisas para desenvolvimento da rede se mudou dos Estados Unidos para a Suíça, onde o inglês Tim Berners-Lee desenvolve o www *(World Wide Web)*. A ideia de Lee era criar um sistema em que todas as informações guardadas nas máquinas pudessem ser interligadas e compartilhadas. O pesquisador entendia a rede como uma infraestrutura de comunicação sem limites fronteiriços e investidores entenderam o potencial econômico da nova ferramenta (Briggs; Burke, 2016).

Porém, a ideia inicialmente proposta era de que o mundo se transformaria em uma aldeia global. Nos primórdios da internet, quando Lèvy (2010) cunhou o termo cibercultura, acreditava-se que a rede fosse proporcionar avanços na comunicação, política, economia, ensejando um círculo virtuoso de desenvolvimento colaborativo. Poucos eram os críticos, contrários à novidade tecnológica. O que se percebeu com o passar do tempo, como enfatiza Morozov (2018), é que o capitalismo se aproveitou

da ferramenta para expandir ainda mais a ideologia de consumo. As empresas do Vale do Silício foram tomando conta do mercado, tornando a ideia de aldeia global em domínio feudal estadunidense. É fácil perceber esta realidade pela expansão dos serviços tecnológicos, nascidos na era da internet, sob domínio de empresas norte-americanas.

Os programas de mensagem instantânea começam a aparecer em 1997 com a entrada no mercado do ICQ, em 2001 o serviço já acumula 100 milhões de usuários. Em 1999, nasce o MSN Messenger, que acaba por reduzir a popularidade do ICQ, já que o MSN era da Microsoft, interligado ao Windows, que a maioria dos usuários tinha instalado em suas máquinas. A primeira rede social nasce em 1997, a SixDegrees permitia a montagem de perfis e inclusão de amigos. Tinha uma interface simplificada e funcionou de 1997 a 2001, só nos Estados Unidos. Em 2002 surge o Friendster e dois anos depois o famoso Orkut, que chegou a registrar 29 milhões de usuários no Brasil. A rede social abriu a oportunidade de formação de comunidades online, antes de ser encerrada em 2011.[1]

O Facebook foi lançado em 4 de fevereiro de 2004 por Mark Zuckerberg, Dustin Moskovitz, Chris Hughes e Eduardo Saverin. A rede social atingiu a marca de 1 milhão de usuários em dezembro do mesmo ano. A partir de 2006, o Facebook oferta o App para celular e começa a atualizar o *feed* com notícias. O botão de *likes* é acionado em 2007 e a sociedade vai se rendendo à validação da audiência. Em 2011, o Facebook aglutina o serviço do MSN e em 2012 comprou o Instagram – rede social criada em 2010, baseada em compartilhamento de fotos, que estava fazendo sucesso no mundo todo. O investimento foi de US$1 bilhão. Dois anos depois, o Facebook adquire por US$19 bilhões o WhatsApp – serviço de mensagens instantâneas, que foi desenvolvido em 2009. Em 2021, a rede social tinha cerca de 2,3 bilhões de usuários conectados ao redor do globo (Facebook, 2021).

Nota-se que a evolução do Facebook foi rápida. Em cinco anos a empresa já dominava as relações sociais digitais do mundo nos quatro aplicativos mais utilizados para conversas instantâneas online e interações pessoais no ciberespaço. Desde que foi lançado, o Facebook admitiu que utilizava o app para testes de física social. A empresa afirmava que fazia uso desta experimentação para conhecer melhor o

---

[1] A evolução das redes sociais e seu impacto na sociedade. Disponível em: https://canaltech.com.br/redes-sociais/a-evolucao-das-redes-sociais-e-seu-impacto-na-sociedade-parte-2-108116/ Acessado em 06/07/2021.

usuário e com isso aperfeiçoar o aplicativo. Mas aperfeiçoar em que sentido? Percebe-se um foco na melhor distribuição de publicidade, visando maior rentabilidade aos anunciantes. Desta forma, a propaganda se transformou no modelo de negócio da internet (Morozov, 2018).

Outra rede de relacionamento social que nasceu com a proposta de funcionar como uma arena pública, global, de discussão de ideias foi o Twitter, fundado em março de 2006. Avaliado em US$3,7 bilhões, em 2020, a empresa propaga a ideia de que o mundo aprenda rápido, para solucionar problemas comuns, com diversidade de opiniões, informações e perspectivas. Mas como nem só de discussão de ideias vive o mundo, a cultura da empresa enfatiza que as pessoas devem ter estas informações para consumir, criar, distribuir e ter acesso a bens midiáticos de seu interesse, ou seja, consumidores preparados para o comércio global online. Por fim, institui o pensamento de que juntos os cidadãos têm condições de fazer o bem coletivo. Mas de que coletivo estamos falando? Talvez os 196 milhões de usuários que subscrevem a rede (Twitter, 2020a).

Desde que chegou à casa das pessoas, há três décadas, a internet evoluiu bastante e passou por três etapas importantes: Web 1.0, focada apenas na transferência de documentos, a Web 2.0, voltada ao relacionamento das pessoas e a Web 3.0, baseada em coleta de dados. Hiremath e Kenchakkanavar (2016) e Di Felice (2021) explicam o que cada uma destas etapas traduzem:

- Na Web 1.0, que é compreendida entre o início dos anos 1990 até 2000, tem poucos programadores que fazem as páginas para usuários. Estas páginas ofertavam quase nenhuma interação entre site e usuários. As conexões eram feitas via cabos telefônicos e modens, que foram rapidamente se modernizando. Mesmo ainda muito rudimentar, nesta fase dava-se início às transformações sociais proporcionadas pelas interações à distância no ciberespaço.
- Na Web 2.0, entre 2000 e 2005, o foco está centrado nas relações e interações pessoais. O usuário não é apenas Leitor, ele já contribui com o conteúdo, começa aqui a ideia de internet participativa. A partir dos anos 2000, com o advento da banda larga, a internet passa por uma mudança qualitativa. Os cabos de fibra óptica, que fazem parte da infraestrutura de transmissão, dão suporte a um aumento exponencial de capacidade de armazenamento de informação, pontos e canais de transmissão. A nova arquitetura abriu a

possibilidade de armazenamento em nuvem e acesso não só via computadores, mas também smartphones e tablets.

- A Web 3.0, termo cunhado em 2006, é a Internet que transforma os dados em informações que podem ser utilizadas para diversos fins, mas está centrada principalmente no interesse comercial. O incremento da conexão no terceiro modelo faz a extensão do processo interativo englobando às coisas e objetos, via radiofrequência (RFID). É a chamada internet das coisas entrando em ação. As informações coletadas pela interação humana com os objetos conectados à rede dão origem a um novo tipo de medida incalculável, que só é possível processar na forma de algoritmos, nasce o conceito de *big data*.

Vários críticos do universo digital afirmam que a rede mundial de computadores não trouxe apenas avanços para a sociedade. Morozov (2018) é um dos pesquisadores que entendem a rede como “um emaranhado confuso de geopolítica, finança global, consumismo desenfreado e acelerada apropriação corporativa dos nossos relacionamentos mais íntimos” (p. 7). Mas o que são estes entes poderosos, que estão a ameaçar soberanias nacionais? Por que cresceram em tamanho e poder os oligopólios que dominam o universo online? Estas são as questões que serão tratadas na próxima seção desta pesquisa.

1.2 Definição de plataformas

O advento do comércio eletrônico estabeleceu o ponto de partida para a criação das plataformas digitais como são conhecidas na sociedade contemporânea. Este processo começa em torno dos anos 2000. Grandes corporações à época como Microsoft, Cisco e Intel forneceram aos pesquisadores uma primeira versão para definir o que seriam as plataformas: “mercados de dois lados” – as plataformas disponibilizam o ambiente online para que desenvolvedores de conteúdo oferecessem seus produtos e os consumidores acessassem o ciberespaço em busca de adquiri-los. Eram entendidas apenas como conduítes dos relacionamentos entre fornecedores e consumidores de produtos ou serviços online. Portanto, não admitiam, a possibilidade de serem responsabilizadas pelo conteúdo postado porque se intitulavam apenas como intermediárias (Poell; Nieborg; Van Djick, 2020).

No período compreendido pelo conceito de Web 2.0, o ambiente online já era visto como apropriado para o desenvolvimento de empresas interessadas no mercado

consumidor que se apresentava lucrativo. Se desenvolveram neste período, em torno de 2005, redes sociais digitais como Youtube, Facebook, MySpace e Twitter. As plataformas, neste período, agruparam as condições ideais para organizar a atividade econômica das empresas, com público-alvo delimitado. A infraestrutura já era pensada para esta finalidade de "interações personalizadas entre usuários finais e complementadores, organizadas por meio de coleta sistemática, processamento algorítmico, monetização e circulação de dados" (Poell; Nieborg; Van Djick, 2020, p. 04).

Por conta desta característica das plataformas de serem compreendidas como infraestruturas de distribuição de conteúdo, pesquisadores como Gillespie (2018) levantaram uma questão: seriam as plataformas também produtoras de conteúdo? Neste período subsequente, além de armazenar, elas já interferiam e transformavam o conteúdo produzido pelos usuários em algo mais atrativo. Faziam a curadoria do conteúdo, modificando o original, editando e distribuindo para pessoas que pudessem se interessar mais pelo produto ou serviço ofertado. Numa visita a uma plataforma é possível observar que a disposição do conteúdo é feita em listas de *trending topics*[2], organizadas em páginas iniciais de forma que os temas atraiam cada vez mais usuários e os mantenha na plataforma.

Para Bostoen (2018) é preciso compreender o que as plataformas fazem, para definir o que elas são. Para o autor, elas não passam de ambientes online de busca e associação - que podem estar ligadas a relacionamentos interpessoais, ou então comerciais, na compra e venda de produtos ou serviços. Morozov (2018) classifica as plataformas como parasitas digitais, porque elas dependem de serviços adjacentes que criam relações sociais ou econômicas. Ao dominar um setor, as plataformas digitais influenciam o mercado daquele produto ou serviço. A maior parte das livrarias, por exemplo, fechou depois que a Amazon entrou e dominou o setor editorial. "Quase todas as plataformas são monopólios, impulsionados pelos efeitos em rede gerados pela operação de um serviço que se torna mais valioso à medida que aumenta o número de usuários" (p. 60).

Quando a atenção se volta ao tratamento das informações, as plataformas digitais podem ser compreendidas como uma "instituição sociocultural da

[2] Trending topics são os assuntos mais comentados na internet, geralmente são acompanhados pelo sinal de #, que é usado para categorizar assuntos, foi inventado por Chris Messina em 2007.

comunicação" (Mintz, 2019, p. 101). A afirmação está baseada no fato de que a internet não seria apenas um aparato tecnológico no qual a informação é disseminada via produtos da mídia, mas sim um sistema que possui regras rígidas de distribuição de conteúdo via governança institucional.

Muitos pesquisadores, inclusive, entendem as plataformas digitais como sistemas de software integrados, que fornecem novos modelos de negócio, com condições para redes sociais e empresas de comunicação organizarem os atores sociais envolvidos na produção midiática para comércio multifacetados e escaláveis. A informação se transformou em ativo de mercado. Ganha mais quem tem maior número de cliques. Perde-se de vista o interesse público, ganha espaço o interesse do público (Flew; Martin; Suzor, 2019).

Morozov (2018) alerta que em geral as plataformas digitais oferecem facilidades para direitos públicos conquistados ao longo de anos de luta, como liberdade de expressão, segurança e transporte. Esta oferta vem empacotada numa embalagem mais eficiente, porém sem garantias públicas, porque é fornecida por setores privados. Observa-se até aqui que as plataformas evoluíram de mercados de dois lados para ambientes multifacetados de troca de informação, relacionamento, coleta de dados e comercialização.

Burke (2003) faz uma diferenciação entre informação e conhecimento, entendendo a primeira como algo cru, em estado primário e o segundo como algo cozido, trabalhado ao longo do tempo. Deste conceito, infere-se que as plataformas digitais podem ter experimentado o processo de evolução da informação, apurada, trabalhada até se transformar em conhecimento com aplicação. No início, as plataformas coletaram informações cruas de seus usuários, monitorando sua navegação, por meio dos *cookies*. Encontraram novas formas de coletar todo tipo de informações, trabalharam os dados, transformaram tudo isso em conhecimento e aplicaram suas inferências para ganharem novos espaços e mercados.

Um estudo feito pela Organização das Nações Unidas (ONU), mostrou que mais da metade da população mundial está conectada à internet, somando 4,1 bilhões de usuários[3]. Pode-se afirmar que a sociedade contemporânea enfrenta uma dependência das plataformas digitais. O ecossistema baseado em plataformas foi

[3] Uso de internet no mundo. Disponível em: https://news.un.org/pt/tags/uso-de-internet-no-mundo Acessado em 06/07/2021.

criando suporte para que todo tipo de conteúdo pudesse ser acessado, adquirido e compartilhado em diferentes formatos (texto, áudio ou vídeo) em sua base de distribuição de produtos e serviços. Atividades da vida cotidiana foram transportadas aos poucos para o ciberespaço. O direito de todos à informação e comunicação na sociedade contemporânea passa pelas plataformas de relacionamento digitais (Cozzolino; Corbo; Aversa, 2021).

Rüdiger (2016) atesta que as mídias sociais e as empresas de mídia se renderam como “criaturas da indústria cultural em que se converteu boa parte do sistema capitalista” (p.35). A proposta positivista do século XIX, de se viver às claras, sem segredos, colocada em prática pelas plataformas de mídias sociais, deu ao aparato tecnológico a possibilidade de coletar informações voluntárias, que não seriam anteriormente pensadas nem pelos regimes totalitários. As infraestruturas tecnológicas transformaram sujeitos em marcas, na sociedade neoliberal. As pessoas são objeto de consumo e têm de aprender as regras de marketing para se autopromover. Redes sociais criam ambientes de reverberação de identificação. Os perfis se assemelham, forjando uma sociabilidade autista, na qual o sujeito se reconhece no seu seguidor e vice-versa.

O autor reconhece fatores positivos sobre as plataformas de mídias sociais como: “expansão do conhecimento, novas oportunidades de sobrevivência econômica e emancipação de contextos heterônimos para alguns grupos sociais” (Rüdiger, 2016, p.37). Porém, duvida que a sociedade do século XXI seja capaz de romper com o sistema capitalista e tornar as redes sociais um ambiente livre da indústria cultural. Nota que os produtores de conteúdo pouco se importam de serem vendidos pelas plataformas a seus anunciantes, na verdade, estão dispostos a ampliar a distribuição de seus bens culturais, para gerarem mais monetização. Até mesmo a militância, que poderia fazer a resistência ao sistema, migrou para as redes e cada vez mais se distancia das manifestações no mundo físico.

Neste contexto ultra conectado a mídia se molda ao meio eletrônico e se reinventa, obedecendo à nova ordem de mercado, ditada pelas plataformas digitais. As notícias são veiculadas em texto, áudio e vídeo, voltadas a nichos cada vez mais delimitados, com foco em algoritmos de distribuição que garantam bom ranqueamento nas plataformas de busca. Quanto mais próximo do topo dos resultados, melhores os números de acesso e consequentemente maior a “monetização” do conteúdo. A

influência anteriormente propagada pela mídia sobre o corpo social precisa de uma análise diferenciada neste novo ambiente (Mintz, 2019).

O impacto da evolução das plataformas digitais na mídia pode ser medido pela migração da verba publicitária dos meios de comunicação de massa tradicionais analógicos para os digitais. Em 2019, nos Estados Unidos, o digital ficou com US$ 129 bilhões do mercado de propaganda, enquanto os veículos de TV, rádio e jornal obtiveram US$ 109 bilhões da verba publicitária.[4] Anuncia-se mais no meio digital porque a comercialização de serviços e produtos também está migrando para as plataformas digitais. Além disso, os algoritmos de leitura de dados ganham eficiência na entrega de propaganda a usuários mais propensos a consumir.

Desde 2017, o Facebook, por exemplo, vem trabalhando formas de melhorar a experiência de compra dos usuários, com possibilidade de envio de ofertas até mesmo via Messenger, o aplicativo de mensagens instantâneas. O conteúdo produzido por terceiros é aproveitado pela plataforma para gerar tráfego de navegação. Os *posts* são relevantes, tratam de saúde, empreendedorismo e o gatilho de venda está inserido naquilo que poderia ser reconhecido apenas como notícia. A informação é apenas embalagem para a propaganda, uma camuflagem de comércio na comunicação. É como um serviço de assistente pessoal digital que vai atender às necessidades do consumidor (Zuboff, 2021).

Mintz (2019) sugere que as plataformas se aproveitam desta nova forma de relacionamento para centralizar acessos, compartilhamento de dados e otimização de publicidade. Relações sociais, de trabalho e comércio passam pelas plataformas. Isso tudo é possível porque o fluxo de informação e comunicação está centralizado nas plataformas digitais, na sociedade contemporânea. É sobre isso que trata a próxima seção.

1.3 Comunicação em rede

A administração de reputação, relacionamentos pessoais e profissionais está contida em banco de dados. O humano e o digital estão unidos de uma forma que o diálogo passa pelo suporte tecnológico seja na discussão de ideias, opiniões ou até

[4] *Digital Advertising in the US is finnaly bigger than print and Televison* Disponível em: https://www.vox.com/2019/2/20/18232433/digital-advertising-facebook-google-growth-tv-print-emarketer-2019 Acessado em 15/09/2021.

mesmo na criação de moedas que não foram emitidas pelos bancos (*criptomoedas*). Muito mais que uma rede de inteligência coletiva, a internet é uma rede que, “por meio de dispositivos móveis, *softwares*, sensores, constitui o ambiente dinâmico em que vivemos e interagimos todos os dias” (Di Felice, 2021, p. 33).

O processamento estático da fonte de informação, que passava por um transmissor e era entregue a um receptor em seu destino, evoluiu na era da internet das coisas passando pelo código do *software*, sendo processada pelos algoritmos, entregue via sensores, armazenada em dados e aplicada nas plataformas. De acordo com Di Felice (2021), os modelos analógicos da comunicação eram inspirados nos sistemas industriais, numa relação semelhante ao processo de produção em massa, já a comunicação em rede desafia este pensamento, propondo uma nova arquitetura informacional.

O sujeito comunicacional contemporâneo não se relaciona centrado em um local específico, um território predeterminado. O ato de comunicar evoluiu ao ponto de pensarmos redes complexas constituídas por seres humanos, dados, sensores, softwares e até mesmo objetos inanimados ligados às arquiteturas informativas. “A essa ideia de habitar, humana, natural e semântica, sucede aquela de um habitar comunicativo reticular, cuja forma é atópica, ou seja, emergente e conectiva” (Di Felice, 2021, p. 47). A dimensão da antiga pólis grega, ou então as cidades da era industrial, tem pouca relação com a realidade da sociedade envolta no ambiente digital.

Lollini, Farley e Lèvy (2019) demonstram como a comunicação na era das plataformas digitais gerou uma nova forma de inteligência coletiva. A rede criou um sistema de desaparecimento físico das barreiras geográficas. Abriu espaço para uma comunicação intermediada pelo ambiente digital, onde a memória coletiva é retida e um arquivo pode ser incrementado e acessado, teoricamente, por qualquer pessoa. “Tem ainda a comunicação de muitos para muitos e a conexão não somente entre pessoas, mas também de documentos” (p. 06). Esta realidade cria duas dialéticas concomitantes a do individual e coletivo e ao mesmo tempo a da memória coletiva e comum.

Apesar da ideia geral ser positiva, no sentido de as plataformas digitais oferecerem um banco de dados que se expande exponencialmente, este é um sistema ainda opaco e aberto a questionamentos. Lollini, Farley e Lèvy (2019) veem, porém, a necessidade de trabalhar no sentido de transformar o ciberespaço em somatória de

esforços dos indivíduos pelo todo, numa perspectiva de inteligência coletiva reflexiva. Uma das perspectivas é tornar as comunidades locais fortes, por meio da comunicação proporcionada pelas redes sociais, como os grupos do Facebook, por exemplo. Afinal, antes mesmo do advento das redes sociais digitais, o ser humano sempre buscou pela comunicação.

Neste ambiente extremamente conectado da vida, com a possibilidade da comunicação global, sem fronteiras, muitos questionam até mesmo a noção de pertencimento pátrio. Castells (2018) teoriza novos parâmetros para a sobrevivência dos Estados-Nação em um ambiente globalizado baseado nas plataformas que revolucionaram o compartilhamento da informação, com comunicação e comercialização em escala global. Estes Estados-Nação enfrentam um desafio identitário em um sistema de "globalização da riqueza e do poder, identificação da cultura e representação" (p. 23).

A observação de Castells (2018) tem como base a formação da União Europeia como bloco econômico, com a necessidade de os Estados-Nação participantes abdicarem de parte de sua soberania para tomada de muitas decisões de forma conjunta. As duas últimas décadas trouxeram transformações políticas por conta da revolução das tecnologias da informação e comunicação, criando a política informacional. Com um celular na mão qualquer cidadão tem o poder de expor uma irregularidade praticada por um político ou então ter acesso à divulgação de mais um escândalo praticado com dinheiro público.

De acordo com o Instituto Brasileiro de Geografia e Estatística (IBGE), 90% da população brasileira já tinha acesso à Internet, em 2021, sendo que 99,5% dos usuários acessam a rede via celular.[5] Uma pesquisa feita pela empresa de segurança digital Kaspersky, em parceria com a *We are Social*, em 2020, mostrou que 83% dos usuários da internet têm algum perfil nas plataformas de mídias sociais. Eles estão distribuídos desta forma: 66% têm conta no Facebook, 54% no Youtube, 45% no Instagram e 40% no Twitter.[6] Na sociedade da informação, a conexão se configura

---

[5] Internet já é acessível a 90% dos domicílios do país em 2021 Disponível em: https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/34954-internet-ja-e-acessivel-em-90-0-dos-domicilios-do-pais-em-2021#:~:text=Internet%20chega%20a%2090%2C0,%25%20para%2092%2C3%25. Acessado em 28/09/20222.

[6] Social credits and security: embracing the world of ratings. Disponível em: https://www.kaspersky.com/blog/social-credits-and-security/ Acessado em: 29/06/2021.

por meio das mensagens trocadas, com geração de conteúdo próprio ou compartilhado de terceiros.

Mas o que será que impele o ser humano a compartilhar um conteúdo? Entre os estudiosos do marketing, o termo para conteúdos propagáveis é aderência, ou seja, aquilo que o indivíduo lê, ouve ou assiste, que gruda e ele sente a necessidade de passar para frente. Jenkins, Ford e Green (2015) reforçam que são estes conteúdos chiclete que geram cliques, aumentam audiência de plataformas e consequentemente as vendas. Pensando nesta lógica, muitas plataformas digitais, como o Twitter, por exemplo, criam mecanismos que tornam o compartilhamento de informação uma ação facilitada. Assim, ao se deparar com um assunto interessante, basta ao usuário apertar um botão para que ele siga seu tráfego na rede.

No Brasil, o compartilhamento de informações pelas plataformas de mídias sociais vem aumentando ano a ano. Uma pesquisa realizada pelo Instituto DataSenado revelou que 58% dos brasileiros admitem que compartilham informações via redes sociais.[7] Muitos destes compartilhamentos têm cunho político. Uma outra pesquisa feita pelo Instituto, em 2019, averiguou que 83% dos brasileiros acreditavam que o conteúdo compartilhado nas redes sociais influenciava a opinião das pessoas. O levantamento mostrou que 79% dos entrevistados utilizaram o WhatsApp para se informar. Pelo menos 83% admitiram que já identificaram alguma informação falsa.[8] Uma outra consulta popular feita pelo DataSenado demonstrou que mais de 40% dos eleitores entrevistados admitiram ter decidido o voto com base em informações obtidas em redes sociais.[9]

Por conta da relevância das plataformas de mídias sociais na tomada de decisão dos eleitores, os políticos têm cada vez mais se utilizado deste meio de relacionamento social online. “Barack Obama utilizou redes sociais como Twitter,

---

7 Maioria dos brasileiros apoia a criação de uma lei contra fake news. Disponível em: https://www12.senado.leg.br/institucional/datasenado/materias/pesquisas/maioria-dos-brasileiros-apoia-a-criacao-de-uma-lei-contra-fake-news Acessado em: 29/06/2021.

8 Mais de 80% dos brasileiros acreditam que as redes sociais influenciam muito a opinião das pessoas. Disponível em: https://www12.senado.leg.br/institucional/datasenado/materias/pesquisas/mais-de-80-dos-brasileiros-acreditam-que-redes-sociais-influenciam-muito-a-opiniao-das-pessoas Acessado em: 28/06/2021.

9 Redes sociais influenciam voto de 45% da população, indica pesquisa do DataSenado. Disponível em: https://www12.senado.leg.br/noticias/materias/2019/12/12/redes-sociais-influenciam-voto-de-45-da-populacao-indica-pesquisa-do-datasenado Acessado em:28/06/2021.

Facebook e YouTube para comunicar-se e interagir com os eleitores.” (Camargo; Magnoni; Miranda, 2018, p. 115) Nos Estados Unidos, a utilização das plataformas em campanhas políticas era uma realidade desde os anos 2.000. Por aqui, no Brasil, a utilização se deu principalmente nas duas últimas eleições, primeiro para presidente e governadores em 2018 e depois, no ano de 2020, para prefeitos e vereadores.

Um levantamento feito por Camargo, Magnoni e Miranda (2018), mostrou que os conteúdos compartilhados pelos políticos no Brasil referem-se principalmente a notícias publicadas pela mídia profissional - como pesquisas; os comitês partidários também disponibilizam informações de campanha - com vídeos e visitas políticas a localidades; e ainda participação do eleitor comentando as postagens. Diante desta migração da comunicação para o universo online, as redes de relacionamento social digital têm uma grande influência na forma de pensar e exercer a política.

Os rituais da participação representativa ganharam novos contornos. Meios de comunicação de massa, como a TV e o rádio, respeitam uma série de regras, instituídas pelo Estado, por meio de legislação, que institui parâmetros do que é possível ser veiculado e de que forma este conteúdo vai chegar ao público. Porém, na internet, as regras de governança são nebulosas e precisam ser tratadas. Este é o assunto da próxima seção.

1.4 Objeto de regulação das plataformas e desafios

A discussão sobre a regulação da internet não é nova, desde o World Summit of Information Society (WSIS), em 2005, o assunto vem sendo discutido. Um dos pontos apontados pela Organização para a Cooperação e Desenvolvimento Econômico, OCDE, é a evolução da noção de responsabilidade dos intermediários da internet, as plataformas digitais, que inicialmente são definidos pela instituição como ambientes que proporcionam o encontro para negociação de terceiros. Esta era a definição, no princípio, que permitia a discussão de responsabilização das plataformas pelo conteúdo. Porém, a definição de plataforma evoluiu para um espaço compartilhado pelos aplicativos, em que os usuários podem transportar suas atividades e gerar valor. Como se percebe um *framework* mais dinâmico precisa ser discutido (Belli, Francisco; Zingales, 2017).

Padovani (2005) relembra que o debate sobre o acesso à informação e comunicação como direito básico de todo cidadão vem dando passos de evolução

desde 1948, quando foi reconhecido pela ONU na Declaração Universal dos Direitos Humanos. As discussões da década de 1970, que deram origem ao Relatório McBride, em 1980, traçaram parâmetros para que o fluxo de informação e comunicação global pudesse ser desenvolvido. Porém, o que se percebe é que o tema segue com desafios ainda maiores a partir do advento da internet, em escala comercial, a partir da década de 1990. As discussões do WSIS trouxeram à tona a necessidade de endereçamento das desigualdades e lacunas tecnológicas que as nações com menor poder econômico enfrentam na sociedade da informação, ficando à margem do processo de desenvolvimento, dependentes dos oligopólios das plataformas digitais.

O que se percebeu a partir do desenvolvimento e evolução das plataformas digitais foi um novo paradigma de redes de poder e riqueza, baseados na comunicação em escala global. Esta nova realidade trouxe consigo um estreitamento entre os processos políticos e comunicacionais, obrigando governos a mudarem suas formas de agir porque as empresas transnacionais, donas das plataformas digitais, influenciam cada vez mais os sistemas econômicos globais por meio dos setores de informação e comunicação. O WSIS chamou a atenção para o fato de que na sociedade da informação há questões transnacionais da comunicação que são capazes de despertar o debate com reflexos em âmbitos locais (Padovani, 2005).

Em 2014, o Institute for Information Law, da Universidade de Amsterdam, fez um relatório sobre regulação de plataformas digitais especialmente para a UNESCO. Dois anos depois, foi apresentado o relatório sobre liberdade de opinião e expressão, pelo Center for Law and Democracy´ s Recommendations on Responsible Tech, também para a UNESCO. Em 2017, o Council of Europe’s fez uma série de recomendações com relação à forma de ação das plataformas digitais. O assunto é tema de um comitê permanente da ONU, o Dynamic Coalition on Platform Responsability, que discute a responsabilidade das plataformas digitais com relação a aspectos técnicos, legais, sociais e econômicos (Belli, Francisco; Zingales, 2017).

Nesta discussão Belli, Francisco e Zingales (2017) apontam que existe uma separação sobre a regulação das plataformas, que exclui provedores de internet. Os provedores são encampados pela indústria das telecomunicações e obedecem a um outro regramento. Mas um ponto na oferta do serviço de provedores que influencia as plataformas está na velocidade do sinal para serviços de *streaming* e este aspecto em questão é entendido como tema de discussão em questões regulatórias.

Há basicamente duas vertentes quando o assunto é regulação das plataformas digitais. Entre os pesquisadores há aqueles que pregam a total liberdade e os que propõem a imposição de uma série de limitações. Os estudiosos em prol da mínima intervenção justificam que quando há problemas relacionados à competitividade no setor, o próprio mercado se corrige, outros argumentam que a regulação poderia dificultar o ambiente de inovação, há ainda quem acredite que não deveria haver uma "Lei das plataformas". Os pró-regulação são divididos entre os que entendem a necessidade de parâmetros para garantir a competitividade, outros que defendem a aplicação de Leis já existentes e ainda os que julgam necessário a criação de um novo regramento para o setor (Bostoen, 2018).

Bostoen (2018) observa que a maior parte dos governos mundiais têm como base dois princípios básicos para regulação: neutralidade e justiça. Estes princípios já foram utilizados anteriormente, como por exemplo na questão dos provedores de internet, com regras não discriminatórias para serviços de *streaming* na Europa e Estados Unidos. Com relação à neutralidade de rede, os objetivos "não incluem apenas regras relacionadas à competição, mas também a objetivos como pluralismo da mídia e liberdade de expressão" (Bostoen, 2018, p. 7). Com relação ao princípio da justiça, o debate se debruça sobre a necessidade de que as plataformas ofereçam seus serviços de boa-fé, sem prejudicar seus usuários finais ou parceiros comerciais.

Para isso, deveria haver uma separação entre resultados de buscas orgânicas, patrocinadas e referentes ao próprio ecossistema de serviços da plataforma. Neste sentido, três motivos básicos poderiam justificar a regulação: 1) o crescente poder que vêm ganhando; 2) a relação assimétrica com relação aos usuários e parceiros comerciais e, ainda, 3) a falta de mecanismos que estabeleçam uma competição justa no ambiente virtual. Diante desta constatação, De Lima *et al.* (2020) apresentam os objetos pelos quais as plataformas deveriam ser reguladas, que seriam gestão de conteúdo; relações econômicas; e, segurança de dados.

Gillespie (2018) é um dos críticos do crescente poder dado às plataformas digitais. Para o autor, a decisão do que pode ou não ser publicado ou compartilhado nas plataformas não deveria ser ofício das grandes empresas da tecnologia. O regramento do que é veiculado no ciberespaço deveria estar vinculado a decisões que compreendem parâmetros pré-estabelecidos para todos. "Usuários não deveriam acreditar que a entrega da regulação às plataformas fosse garantir que elas

resolveriam as demandas perfeitamente, no tempo correto, com imparcialidade" (Gillespie, 2018, p. 01).

As plataformas, principalmente de redes sociais, venderam a ideia de participação popular no discurso público, com liberdade de expressão e informação a quem quisesse se manifestar. No princípio se furtaram ao papel de corresponsáveis por aquilo que era veiculado, se classificavam como conduítes apenas. Porém, a exposição de ideias é o que molda a cultura popular. De acordo com Gillespie (2018), os problemas públicos gerados por este comportamento já são conhecidos:

- Polarização, por conta da personalização de conteúdo feita pelos algoritmos;
- Ações coordenadas de assédio, com campanhas de cancelamento;
- Propagação de desinformação;
- Gameficação de conteúdos na intenção de simular engajamento.

Quando deram início ao processo de moderação dos conteúdos, as plataformas não mencionaram quais parâmetros seriam usados. Belli, Francisco e Zingales (2017) reforçam que o Council of Europe´s recomenda às plataformas que retirem do ar conteúdos ilegais, com base em Leis do bloco e Leis dos países. Neste sentido, as plataformas vêm assumindo a posição de autorreguladoras dos conteúdos, que seria uma função do direito público e não privado.

Gillespie (2018) argumenta que o ambiente é nebuloso, com regras que são decididas a portas fechadas e que o público tem pouco ou nenhum acesso. Em todo o mundo há discussões relacionadas a diversos conteúdos postados nas plataformas digitais, principalmente de redes sociais, tais como: pornografia, violência, misoginia, homofobia, racismo, bullying, extremismo religioso e político, entre outros. E a moderação vem sendo feita sob o crivo das plataformas. Esta é a tarefa na qual elas empregam um número crescente de trabalhadores.

As formas pelas quais as plataformas fazem moderação variam: podem remover, filtrar ou suspender o conteúdo; podem recomendar, colocando na página inicial dos usuários, em lista de *trending topics* e sugestões personalizadas; fazem ainda a curadoria, oferecendo na primeira página um conteúdo com o qual estejam alinhadas. Criam assim bolhas, com maior engajamento de usuários, melhor chance de venda de produtos e coleta de dados (Gillespie, 2018).

Em 2016, no governo estadunidense de Barack Obama, as grandes empresas de tecnologia foram impelidas a agilizar processos para identificação de conteúdo de organizações terroristas para retirá-los do ar e reportar aos serviços de segurança

nacional. Mesma época em que os legisladores europeus impuseram às *Big Techs* o prazo de uma hora para retirada do ar de propaganda terrorista, assim que notificadas e ainda 24 horas para retirada de postagens com discursos de ódio. As relações das plataformas com seus usuários e parceiros comerciais há tempos vêm enfrentando um clima de tensão (Gillespie, 2018)

Além das questões relacionadas à regulação do conteúdo, é preciso pensar na produção e venda dos ciberprodutos. O ambiente digital necessita de regras antitruste, que incentivem a competição e inovação, sem criar um sistema que canibaliza atividades econômicas. Quem faz a defesa deste pensamento é Morozov (2018), que alerta para a necessidade de se pensar o mundo sob uma ótica com menor influência do consumismo global e dissolução do Estado, como meta para solução dos problemas sociais. Neste sentido, a regulação das plataformas digitais é uma condição de sobrevivência das economias nacionais, em detrimento da economia globalizada.

Morozov (2018) observa que a referência às empresas da Big Pharma, Big Food e Big Oil, pertencentes respectivamente ao setor farmacêutico, alimentício e do petróleo, sempre é feita de forma pejorativa. Estas seriam empresas centradas apenas no lucro, sem qualquer preocupação social. Diferentemente quando há uma referência às Big Techs, “definido como ‘digital’ ao invés de ‘político’ e ‘econômico’, desde o princípio o debate é conduzido em termos favoráveis às empresas de tecnologia” (p. 29). É como se a evolução que viesse do ciberespaço, por ser digital, fosse sempre positiva.

A redução de competitividade dentro do próprio setor de tecnologia é o sintoma de um problema. O modelo de negócio mostra que pequenas empresas têm sido adquiridas, em seu princípio, pelas grandes empresas que querem eliminar novos *players* do mercado. Não há na Europa, por exemplo, nenhum substituto do Facebook ou do Google. Nota-se o avanço do Vale do Silício sobre as atividades produtivas e econômicas até mesmo fora do ciberespaço. Como a criação da Uber, que prejudicou os taxistas, da Airbnb, que afetou o setor hoteleiro ou da Amazon, que inviabilizou livrarias físicas, “fazendo com que a identidade de consumidor sobrepujasse a de cidadão”. (Morozov, 2018, p. 20)

Em 2014, o Alto Comissariado das Nações Unidas apontou falhas na atuação dos Estados, que têm permitido a violação constante do direito à privacidade de seus cidadãos, esquecendo princípios básicos de direitos humanos. (De Lima *et al.*, 2020)

Em troca de acesso gratuitos a serviços, aplicativos ou então de descontos, usuários concordam com a cessão de seus dados pessoais. Uma pesquisa feita pela Kaspersky, empresa de segurança digital, demonstrou que 43% dos entrevistados admitiram que trocariam dados por descontos ou melhores condições de oferta de serviços online.

Uma das premissas que ficou clara até aqui é que as plataformas se valem da coleta de dados dos usuários e utilizam estas informações para oferecer conteúdo midiático, produtos e serviços que têm maior probabilidade de serem consumidos de acordo com o perfil dos indivíduos. Este sistema causa um efeito de cacofonia, em que as pessoas estão cada vez mais fechadas em suas bolhas e consomem de forma direcionada. Os produtores de conteúdo acabam servindo como força de trabalho indireta, se servem dos dados coletados pelas empresas para entregar produtos consumíveis e neste ciclo, a privacidade de todos está comprometida.

No próximo capítulo são apresentadas as transformações econômicas das plataformas, com domínio dos principais setores de produção e como esta realidade impacta o discurso público, a privacidade e segurança do usuário na rede.

2 – O PODER DAS BIG TECHS

As empresas conhecidas pelo acrônimo GAFAM, que compreende Google, Amazon, Facebook, Apple e Microsoft, dominam não apenas o mercado de tecnologia, mas a economia mundial. Estas empresas trabalham com tecnologia da informação e comunicação primordialmente. Elas estão intimamente ligadas ao cenário político e às esferas decisórias de poder. Nesta tese a análise foca esforços nas redes de mídias sociais, que no princípio, na metade dos anos 2000, representavam um espaço de contato social inicialmente mais direcionado ao entretenimento e, mais recentemente, se transformaram em ambientes contemporâneos de debate e discussão do pensamento público.

Para assinalar a importância destas empresas, foi apresentado um panorama das transformações da indústria cultural, que migrou de um cenário de monopólios de comunicação locais, para oligopólios transnacionais. Neste novo contexto, o capitalismo evoluiu para uma versão tecnológica. Características próprias do sistema econômico, como o individualismo, servem a um ente centralizador, que são as plataformas digitais. O novo quadro implica numa perda de relevância dos governos, por conta de uma dependência econômica em relação às plataformas, que dominam boa parte das relações não apenas sociais, mas também comerciais e trabalhistas.

Para fazer frente a questionamentos judiciais, as plataformas têm criado normas autorregulatórias. Esta é uma medida também para tentar evitar a regulação estatal de suas atividades. As normas apresentadas em seus termos de uso são de adesão obrigatória aos usuários, sob pena de ficarem de fora do ecossistema e serviço oferecidos pelas plataformas. A falta de competição no setor, organização dos produtores de conteúdo e lentidão de ação governamental são fatores que contribuem para que a autorregulação seja uma forma de manutenção de poder pelas plataformas.

Este segundo capítulo traz na seção 2.1 o posicionamento da indústria cultural na versão até 2022. No ponto 2.2 é apresentado o quadro econômico das empresas de tecnologia e sinalizado como alcançaram notoriedade por meio da evolução de seu valor mercantil. Na seção 2.3 é apresentado um quadro da economia política da comunicação no contexto das redes de mídias sociais. A seção 2.4 mostra como as plataformas digitais se valem do conteúdo de terceiros para garantir produção em constante renovação para atrair novos usuários. A seção 2.5 apresenta a prática das

plataformas de coletar dados dos usuários para venda, colocando em risco a privacidade do indivíduo.

2.1 Indústria cultural

A indústria cultural, termo cunhado por Adorno e Horkheimer (2021), no século XX, ganhou uma nova dimensão na sociedade digital. Para Rüdiger (2016) a cibercultura é o estado avançado da indústria cultural e leva seus usuários a duas situações: a primeira é a clausura, pela dependência dos aparatos tecnológicos e a segunda, a experiência vivenciada do consumo midiático em dispositivos móveis. No passado a TV cumpriu esta função, no século XXI a mídia interativa acompanha o ser humano por onde ele for. Não é necessário mais o esforço do estado ou das empresas para divertir as massas, elas mesmo assumiram esta tarefa.

> Os espetáculos da mídia corporativa e a propaganda abominável que essas massas supostamente contestavam se tornaram objeto de sua própria criação, projetando em novo patamar a submissão voluntária a que se haviam imposto durante a primeira era da indústria cultural (Rüdiger, 2016, p. 44-45).

Para Manovich (2018) a maior diferença da indústria cultural de outrora e a contemporânea da internet é a possibilidade de analisar os dados em tempo real. A fase em que a indústria cultural vai ser chamada pelo autor de estágio analítico da mídia. A preocupação principal desta fase é a escala de penetração da cultura digital. No passado, as pesquisas eram feitas por formulários e estavam sempre atrás dos comportamentos de consumo. Nos casos específicos de Facebook e Twitter, a análise de dados oferta conteúdo de mídia mais voltado ao hábito de interação e ainda lista de amigos que melhor se relaciona com os ideais do usuário. Em 1995, a prática de análise de dados teve início e em 2010, quando o Facebook obteve 500 milhões de usuários, ela estava pronta para uso massivo.

As ações da mídia no estágio analítico vão ser divididas em “dois tipos: 1) ações automáticas parcialmente controladas por entradas ou configurações pré-estabelecidas; e 2) ações automáticas não controladas por entradas explícitas do usuário” (Manovich, 2018, p. 481). No primeiro caso, a resposta da mídia vai ser dada por um *input* do usuário, por exemplo, quando ele procura por uma informação em uma plataforma de busca, a entrega do produto vai depender da demanda. Já na segunda opção, a ação da mídia é independente de uma operação do usuário, por

exemplo, a recomendação de um produto, via anúncio, vai chegar ao usuário dependendo do comportamento na rede.

As ações automáticas da mídia são divididas ainda em duas espécies: 1) deterministas – dando sempre o mesmo resultado para o mesmo *input*; ou 2) não deterministas – oferecendo resultados diferentes para o mesmo *input*, dependendo, neste caso, do comportamento do usuário na rede. Na observação de Manovich (2018), a mudança da indústria cultural do século XXI está exatamente na segunda espécie de ações automáticas. As ações não deterministas oferecem para uma mesma demanda resultados diferentes baseados na leitura de dados do usuário, dando a cada um a versão mais próxima daquilo que o indivíduo comumente consome na rede.

Ribeiro e Hebster (2020) apontam as principais diferenças entre os bens materiais, característicos da era analógica, e os imateriais, próprios da indústria cultural digital. Os materiais, por sua natureza, podem ser usados apenas em um determinado tempo e lugar, por uma pessoa ou determinado grupo de indivíduos. Já os imateriais podem ser utilizados de forma síncrona, por qualquer um que tenha a capacidade de reproduzi-los, em qualquer lugar do planeta. No caso dos produtos digitais, intangíveis, a Lei de oferta e procura não se aplica, pois não há escassez de mercado, estão disponíveis na rede para quem tiver condições de acessá-los simultaneamente.

Como bem observou Bolaño (2018), a característica objetiva das tecnologias da informação e comunicação, que tinha em seu princípio um discurso de liberdade, acaba se transformando em mais uma ferramenta para geração de lucro. Na relação capital-trabalho a indústria cultural da era da internet foca em dois pilares: publicidade e programa. O modelo não é diferente do anterior, das mídias de massa, em que o rádio e a televisão se basearam. Esta é a forma como a indústria cultural sustenta a sociedade capitalista, alicerçada no consumo de mercadorias, para as quais têm seus desejos despertados por meio de técnicas psicológicas de venda.

Bolaño (2018) chama a atenção para alguns pontos que devem ser destacados na análise das tecnologias utilizadas para acumulação de capital na sociedade da informação, visível a partir do início do século XXI, fazendo uma diferenciação entre as utilizadas no processo de produção dos bens culturais, para aquelas empregadas em sua distribuição. As primeiras estariam a favor da multiplicação dos bens culturais, de certa forma na tentativa de democratizá-los, retirando deles a aura burguesa de

exclusividade. Porém, ao mesmo tempo, quando se faz uma distribuição em massa dos bens culturais perde-se de vista a valorização daqueles que os criaram, focando-se apenas num mercado consumidor. E assim, “a coisa domina o sujeito” (Bolaño, 2018, p. 139).

Para Rüdiger (2016), porém, a sociedade das redes sociais digitais mesmo tendo a oportunidade de pensar coletivamente não o faz. O aparato tecnológico é transformado em mais uma ferramenta de afirmação individualista. Quem não se insere nas plataformas deixa de participar das redes sociotécnicas. Alguns alcançam sucesso nesta engrenagem, cercam-se de bens de consumo e alimentam o narcisismo coletivo, em que as pessoas perdem as faculdades relacionais. O indivíduo de sucesso expõe seu poder, enquanto quem busca a mesma notoriedade serve de plateia. O que surpreende ou causa estranheza dura pouco, pela velocidade imprimida no ciberespaço. Nesta realidade, “o sentido social é a busca de prestígio sob a forma de popularidade” (p. 42).

Diante deste cenário, Bolaño *et al.* (2020) sinalizam para a transformação da velha indústria cultural, da fase de meios de comunicação de massa, como a TV e o rádio, para a nova realidade da internet. “O barateamento dos equipamentos digitais e a redução consequente dos custos de produção permitiam um crescimento exponencial das ofertas de todo tipo de conteúdo audiovisual, inclusive amadores” (p. 10). Há uma clara desconexão com os antigos detentores dos monopólios de comunicação e os atores da indústria cultural atualizada pela internet estão personificados nas figuras dos donos das plataformas transnacionais.

A mídia globalizada é refletida nos produtos da indústria cultural *high tech* como filmes, séries, livros, música, navegam no ambiente online sem barreiras fronteiriças. Rüdiger (2016) vê nisso um lado positivo, na oportunidade “em termos de expansão do conhecimento, novas oportunidades de sobrevivência econômica e emancipação de contextos heterônimos para alguns grupos sociais” (p. 37). Porém, critica a visão de Jenkins que a sociedade vive ainda a era da economia participativa. Já que o sistema de comércio global é dominado pelas plataformas e são elas que lucram com a exploração do conteúdo alheio. Toda a produção e comercialização dos produtos é pensada para a escala global, de forma que os altos custos de transmissão via satélite, infraestrutura de rede sejam diluídos e o lucro maximizado.

O ecossistema mundial foi pensado para este momento com respaldo do Banco Mundial, Fundo Monetário Internacional (FMI) e Organização Mundial do Comércio

(OMC), assim como de governos, com destaque para os Estados Unidos, principal interessado na manutenção de empresas transnacionais. McChesney (2016) chama a atenção para o fato de que a cultura estadunidense, que já tinha uma grande influência no ocidente, passa a se infiltrar em novos mercados. Um dos sinais desta supremacia na indústria cultural contemporânea pode ser observado na hiper comercialização do sistema midiático globalizado, que é uma característica marcante do mercado estadunidense desde a introdução dos meios de comunicação de massa.

Interessante observar que os novos *players* da indústria cultural (Facebook, Instagram, Twitter, Badu, Google, Amazon) ainda não completaram 20 anos. Os antigos *players* (estúdios de filmes, editoras de livros, emissoras de TV) existem desde o século passado, porém, vêm perdendo hegemonia e viram a necessidade de investir também na leitura de dados. Perceberam que para manter a produção profissional de conteúdo, em contraste à produção de usuários das redes sociais, precisam andar em compasso com a evolução tecnológica. “O que eles analisam e otimizam é principalmente a distribuição, marketing, publicidade, descoberta e recomendações, ou seja, a parte da indústria cultural sobre onde os clientes buscam, compram e usam os produtos culturais” (Manovich, 2018, p. 480).

Segundo Zuboff (2021), a indústria cultural contemporânea seria ainda mais dominadora do que experiências vividas nos séculos XIX e XX. Para a autora, a sociedade do século XXI estaria diante de uma lógica econômica parasítica que, empreendendo uma arquitetura global, busca mudar o comportamento das pessoas. Esta lógica usa o ser humano como matéria-prima em duas condições: num primeiro momento como produtor de conteúdo não vinculado às empresas para gerar constantemente novas ofertas aos usuários; e, num segundo momento, por meio da experiência do usuário, seja com produtos ou serviços que também é transformada em matéria-prima para desenvolvimento de novas ofertas, moldadas de acordo com a Leitura de dados.

Ambas as situações visam a exploração do ser humano para gerar lucro, numa destituição da soberania do indivíduo. A era digital instituiu, para Zuboff (2021), o capitalismo de vigilância. Quem tem a posse dos dados dos usuários vende às empresas que necessitam prever o futuro na geração de novos bens e serviços. “Os capitalistas de vigilância descobriram que os dados comportamentais mais preditivos provêm da intervenção no jogo de modo a incentivar, persuadir e arrebanhar

comportamento em busca de resultados lucrativos" (p. 19). A ideia, portanto, é que os produtos culturais contribuam para que novos comportamentos sejam moldados.

Por isso mesmo, o universo digital cerca as ações e tarefas humanas mais simples do cotidiano com ferramentas que proporcionam a coleta ininterrupta de dados. O detalhamento sobre o funcionamento do capitalismo de plataforma é detalhado na próxima seção.

2.2 Capitalismo de plataforma

É muito difícil imaginar uma empresa que esteja, neste momento, fora do ciberespaço, em especial as redes sociais. O posicionamento digital é condição *sine qua non* para que as empresas consigam fazer negócios. A prevalência das plataformas digitais na economia pode ser traduzida em números. De acordo com a lista da Standard & Poor's 500, um dos indicadores da bolsa de valores estadunidense, as gigantes da tecnologia foram enriquecendo e se tornando as empresas mais valiosas do mundo. Esta evolução pode ser acompanhada no Quadro 1, que traz a lista de 10 empresas mais bem cotadas na bolsa de Nova York, publicada anualmente pela revista Forbes[10].

Quadro 1 – Empresas mais valiosas do mundo

Ranking **S&P 500**	**2010**	**2015**	**2020**
1º	Exxon Mobil Valor: US$ 369 bilhões Setor: petróleo e gás	Apple Valor: US$ 735 bilhões Setor: tecnologia	Apple Valor: US$ 241,2 bilhões Setor: tecnologia
2º	Apple Valor: US$ 296 bilhões Setor: tecnologia	Google Valor: US$ 375 bilhões Setor: tecnologia	Google Valor: US$ 207,5 bilhões Setor: tecnologia
3º	Berkshire Hathaway Valor: US$ 198 bilhões Setor: investimentos	Microsoft Valor: US$ 357 bilhões Setor: tecnologia	Microsoft Valor: US$ 162,9 bilhões Setor: tecnologia
4º	General Eletric Valor: US$ 369 bilhões Setor: variado	Exxon Mobil Valor: US$ 356 bilhões Setor: petróleo e gás	Amazon Valor: US$ 135,4 bilhões Setor: tecnologia
5º	Wallmart Valor: US$ 192 bilhões	Berkshire Hathaway Valor: US$ 349 bilhões	Facebook Valor: US$ 70,3 bilhões

[10] 10 empresas mais valiosas do mundo: hoje x 2010. Disponível em: https://forbes.com.br/listas/2015/06/10-empresas-mais-valiosas-do-mundo-hoje-x-2010/#foto10 e As marcas mais valiosas do mundo em 2020. Disponível em: https://forbes.com.br/listas/2020/07/as-marcas-mais-valiosas-do-mundo-em-2020/#foto10 Acessado em 02/07/2021

	Setor: varejo	Setor: investimentos	Setor: tecnologia
6º	Chevron Valor: US$ 184 bilhões Setor: petróleo e gás	Wells Fargo Valor: US$ 298 bilhões Setor: finanças	Coca-cola Valor: US$ 64,4 bilhões Setor: bebidas
7º	IBM Valor: US$ 182 bilhões Setor: tecnologia	Johnson & Johnson Valor: US$ 278 bilhões Setor: variado	Disney Valor: US$ 61,3 bilhões Setor: lazer
8º	P&G Valor: US$ 180 bilhões Setor: variado	General Eletric Valor: US$ 276 bilhões Setor: variado	Samsung Valor: US$ 50,4 bilhões Setor: tecnologia
9º	AT&T Valor: US$ 174 bilhões Setor: telecomunicações	JP Morgan Chase Valor: US$ 256 bilhões Setor: finanças	Louis Vuitton Valor: US$ 47,2 bilhões Setor: luxo
10º	Johnson & Johnson Valor: US$ 170 bilhões Setor: variado	Facebook Valor: US$ 238 bilhões Setor: tecnologia	MacDonald's Valor: US$ 46,1 bilhões Setor: alimentação

Fonte: Elaborado pela autora com base em lista da Revista Forbes de 2015 e 2020

Num levantamento feito por Fuchs (2021) é possível observar que 21 das 50 maiores corporações transnacionais da contemporaneidade têm como negócio a indústria digital, centrada em comunicação, informação e tecnologia. Em 2019 estas corporações faturaram US$ 2,5 trilhões e acumularam em um ano 3% de toda a riqueza mundial. A partir da análise do capital social acumulado por estas empresas o autor enumerou 10 pontos relacionados às consequências do capitalismo digital na sociedade. São eles:

1. Exploração do trabalho digital e concentração de monopólios da indústria tecnológica;
2. Valorização de uma cultura de individualismo e autopromoção;
3. Criação de uma indústria de monitoramento;
4. Propagação de discursos de ódio;
5. Uso de inteligência artificial que dificulta ao usuário distinguir conteúdos de produção humana e robótica;
6. Desenvolvimento de bolhas ideológicas;
7. Formação de uma indústria da fofoca online, que cria conteúdos feitos para vender;
8. Estímulo ao desenvolvimento de um novo paradigma de vendas, por meio de *influencers* que disfarçam propaganda em conteúdo de entretenimento;

9. Estabelecimento de uma lógica de rapidez e entrega de informação sem debate;
10. Proliferação de *fake news*, que tratam os temas em questão com sensacionalismo.

Rüdiger (2016) concorda com Fuchs (2021) na análise de que há inúmeros problemas causados pelo capitalismo de plataforma e o único jeito de romper com o ciclo de dominação seria o investimento de grupos trabalhando em cooperativas para se apropriarem de fato das redes sociais. Porém, o autor observa que os produtores de conteúdo da sociedade contemporânea pouco têm se importado com o fato de entregarem seus textos, vídeos e áudios para as plataformas, desde que elas coloquem seus produtos em destaque, para que sejam monetizados pela audiência. “Agora, são poucos os que desejam ficar de fora ou por elas não têm interesse” (Rüdiger, 2016, p. 39).

Fica claro na análise de Rüdiger (2016), sobre o capitalismo de plataformas, que este ressignificou ao mesmo tempo o individualismo, característico da acumulação de riqueza aos que fazem sucesso na rede, mas os torna dependentes de uma força maior, sobre a qual não têm nenhum controle. As plataformas a todos dominam, seus interesses são obscuros, “chegando a arrasar a existência entre os mais frágeis e atrasados” (p. 41). Na rede, todos se mostram donos de si, mas na verdade pouco domínio têm sobre suas relações, já que estas são dependentes do algoritmo distribuidor da plataforma.

Para garantir consumo, as plataformas se valem dos dados coletados dos usuários e vão implementando a individualização da experiência de compra. A dificuldade de conceber o sistema, atrapalha legisladores a tratarem de soluções para o problema de consumo direcionado. Com isso, as plataformas foram ganhando espaço e mercado. Acabaram por dominar a economia global. O modelo de negócio iniciado nos anos de 1990 foi utilizando os dados de forma tímida, porém, o emprego de individualização de consumo acabou se tornando a forma que as plataformas encontraram para crescer e se perpetuar no mercado (Mansell; Steinmuller, 2020).

É o domínio exercido pelos algoritmos, que tem encontrado pouca resistência junto aos Estados, talvez pelo atraso tecnológico dos governos. E esta realidade tem um preço alto aos cidadãos. Cientes deste atraso, as empresas de tecnologia oferecem soluções tecnológicas aos governos em troca de dados. Desta forma, conseguem monitorar informações nos serviços públicos. Esta exploração traz

resultados como o aumento no valor de empresas de seguro no mercado de ações. Estas corporações conseguem melhorar seus ganhos, por conta da leitura de dados dos clientes, oferecem serviços sob medida, com resultados mais precisos (Morozov, 2018).

Quanto maior o número de usuários agregados, mais valorizadas são as plataformas. Por isso, muitos serviços e produtos são ofertados de forma gratuita, para garantir o aumento da massa para a coleta, classificação e catalogação de dados. As regras de preço para complementadores (desenvolvedores de conteúdo, empresas e anunciantes) são dependentes das métricas, que mudam constantemente devido à característica volátil deste mercado online, baseado no comportamento do usuário final e número de potenciais consumidores que cresce constantemente. A plataforma evolui com o usuário e cada vez mais desenvolve mecanismos para determinar a predição de mercado futuro (Zuboff, 2021).

A estrutura criada pelas plataformas retroalimenta essa realidade e proporciona a sua perpetuação, baseada na mineração de algoritmos de dados. Pouco interessa o produto ou serviço ofertado, os algoritmos produzidos a partir dos dados coletados durante a interação do usuário com a plataforma é o bem mais valioso da transação. A afirmação de que os dados são o novo petróleo é frequentemente citada no universo da economia contemporânea. A troca do produto por dinheiro vai gerar lucro imediato, porém, a coleta e mineração dos dados compartilhados pelo usuário é que vai determinar a próxima produção de bem midiático ou material que será comercializado (Grohmann, 2020).

Para que as empresas sejam beneficiadas por propagandas direcionadas, as plataformas de mídias sociais foram convertidas em centrais de logística, fazendo a coleta, apuração, classificação e direcionamento de conteúdo via algoritmo de dados. A massa de indivíduos que está utilizando a plataforma vai se encaixando em perfis de algoritmos, para os quais são direcionados conteúdos, são suprimidos outros, têm *posts* deletados, entram em listas de suspensão de contas. Num serviço constante de moderação que desumaniza o ser humano (Gillespie, 2018b).

Nieborg e Poell (2018) destacam que as plataformas moderam a forma como usuários e complementadores se relacionam via interface. Este sistema de governança das plataformas limita a oportunidade que os complementadores ou mesmo os usuários têm de experimentar novas experiências de utilização de bens e serviços em outras plataformas não agregadas. Ao mínimo sinal de competição de

novas plataformas, as grandes empresas da tecnologia se utilizam do poder econômico para adquirir o concorrente antes que este lhe subtraia mercado.

Prática aceita e utilizada pela indústria cultural na lógica de produção customizada de conteúdo consumível, garantindo a máxima distribuição dos produtos midiáticos. Nesta busca por maximizar conteúdo, expondo cada vez mais o usuário a novidades, as plataformas vêm se aproveitando da produção de terceiros para incrementar a experiência do usuário. Porém, no capitalismo de plataforma a busca é sempre por maximizar ganhos e reduzir custos. Nota-se na próxima seção que as redes sociais modificaram o quadro da economia política da comunicação.

2.3 Economia política da comunicação e redes sociais

No arranjo das plataformas, as empresas de mídia competem diretamente com os conteúdos dos usuários. Esta é uma característica deste período pós plataformas, em que qualquer indivíduo pode produzir conteúdo e disponibilizá-lo ao escrutínio público, sem mediação. Porém, "é possível identificar múltiplas instâncias em que esta mediação se manifesta" (Mintz, 2019, p. 103). Como a rigidez na interface de apresentação de conteúdo, a aplicação de algoritmos de distribuição, políticas de consentimento de adesão à plataforma. Há neste ambiente uma migração do poder dos grandes conglomerados de comunicação para as plataformas digitais.

O ambiente das plataformas é altamente interdependente. A infraestrutura de dados cria a linguagem de rede para melhor distribuição de conteúdo, produzido pelos complementadores, que visa atingir o público-alvo. Poell, Nieborg, Van Djick (2020) observam que o consumo da informação determina a expansão da plataforma ou a sua extinção, como é o caso da loja de aplicativos da Apple. Esta concentra todos os aplicativos autorizados para o sistema operacional iOS, que atende aos produtos da empresa como *iphone*, *ipad* etc. Os desenvolvedores dependem da loja virtual para distribuição de seus produtos, enquanto a empresa se apoia nesses complementadores para geração de novos conteúdos, que serão consumidos pelo público final, porém, mesmo interdependente, as relações de poder são desiguais.

Quando as plataformas conseguem reunir muitos produtores de conteúdo, como desenvolvedores de aplicativos, por exemplo, elas concentram o consumo, dificultando a entrada de novos *players* no mercado. Além da dificuldade de novas plataformas entrarem, o produtor de conteúdo sofre com a concorrência dentro do

ambiente que está repleto de outras ofertas. Para saber o que o usuário final quer, a coleta de dados é cada vez maior, há uma necessidade de compra de publicidade, para alcançar melhor posicionamento no ambiente de busca da plataforma e as grandes corporações, como Apple e Google, vão ampliando seu monopólio neste sistema (Poel; Nieborg; Van Dijck, 2020).

Com consumo concentrado e atração de muitos usuários finais, as plataformas criam regras de entrada e permanência dos desenvolvedores de produto. Esta governança passa por algoritmos que determinam a forma como os aplicativos e demais conteúdos serão distribuídos. Este regramento atende à lógica de mercado da plataforma, mudando constantemente para manutenção e ampliação de acesso dos consumidores finais. Poel, Nieborg, Van Djick (2020) apontam que as regras das plataformas são nebulosas e muitas vezes estão em desacordo com a regulação de diversos setores nos países em que oferecem seus serviços.

Bourreau e De Streel (2020) fizeram um estudo para o Centro de Regulação Europeu sobre a política de aquisição das Big Techs*,* na busca por hegemonia de mercado. As empresas conhecidas como GAFAM gastaram 31,6 bilhões de dólares em 2017 apenas em aquisições de *startups*[11]. Entre os anos de 2001 e 2018, a Google, sozinha, adquiriu uma empresa por mês, durante todos os meses no período, totalizando 215 aquisições. Entre 2015 e 2017, as GAFAM compraram 175 companhias. As maiores negociações foram:

- Facebook comprou o WhatsApp, em 2014, por US$ 19 bilhões;
- Google assume o controle da Motorola Mobility, no mesmo ano, por US$ 12 bilhões;
- Microsoft adquire o LinkedIn, em 2016, por US$ 26 bilhões.

Como demonstra o relatório, há um risco muito grande à inovação e competição em um mercado tão concentrado. Os novos empreendedores precisam trabalhar sobre a lógica das plataformas para as quais vão subscrever produtos e se alguma ideia disruptiva aparece, logo recebem uma proposta irrecusável. Muitos trabalham inclusive com esta lógica, fazer um produto ou serviço inovador que chame a atenção das grandes plataformas, para ser comprado por uma fortuna. Há uma barreira de entrada a novos *players* de mercado, permanecendo os mesmos no topo da cadeia.

---

11 O termo *startup,* do inglês, denota uma empresa iniciante do setor de tecnologia. A ideia é que esta empresa iniciante tenha um modelo de negócio repetível, escalável e sustentável.

Problemas verificados que o Centro Europeu de Regulação vem tentando trabalhar (Bourreau; De Streel, 2020).

A comunicação se transformou em uma *commodity* do sistema econômico de plataformas globais. Neste sentido, “informação, educação, política, cultura, entretenimento, assim como condições de vida e trabalho, são constantemente comercializados como produtos” (Knoche, 2021, p. 326). E as implicações desta nova realidade são o recrudescimento das práticas capitalistas em setores anteriormente dominados pelo Estado, como a política e a educação. Sendo a educação a última a ser abarcada pelas plataformas digitais no período de pandemia da Covid-19, a partir de março de 2020.

A partir desta constatação, Knoche (2021) elenca os problemas gerados e alerta: a privatização, desregulação e comercialização de setores como rádio, televisão, telecomunicações e internet estão evoluindo rápido; a comercialização de conteúdo, inclusive jornalístico, já é uma realidade deste mercado; pode-se notar um estreitamento das relações entre a indústria da mídia e o Estado; e uma participação crescente da mídia na transformação econômica gerada pelo capitalismo digital. O alinhamento da indústria midiática à economia global é parte decisiva no desenvolvimento e evolução do capitalismo digital, proporcionando a circulação de bens, por meio de propaganda de consumo; garantindo a legitimação da mensagem ideológica da era globalizada; e ainda, promovendo a retroalimentação do sistema, pela força de trabalho que consome seus próprios bens.

Plataformas de notícias encontraram, inclusive, uma forma de agregar valor aos dados de navegação para alcançar maior engajamento e com isso, melhorar a monetização de seus conteúdos. Buzz Feed, Huffington Post e Upworthy foram pioneiras nesta prática. Perde-se de vista o interesse público da notícia, base do jornalismo analógico, e foca-se no interesse do público, do jornalismo digital. A produção de reportagens vai obedecer à demanda de mercado. A decisão de produção começa em uma pesquisa nas plataformas de busca, para saber quais são os *trending topics*[12]. A partir disso, a notícia é produzida no formato – texto, áudio ou vídeo – mais propenso a ser consumido. Após a publicação, o monitoramento dos

[12] *Trending Topic* é o termo designado para os assuntos com maior volume de interesse dentro das plataformas, num período determinado do tempo. Geralmente são agregados por *hashtags*, que ajudam o usuário a localizá-los e entrarem na discussão.

dados gerados pelo acesso ao assunto vai ajudar a saber se o conteúdo funcionou (Nieborg, Poell, 2018).

A avaliação depende de métricas como compartilhamento, comentários e curtidas do conteúdo na plataforma em que foi postado. Nieborg e Poell (2018) vão chamar este ciclo de “dependência de plataforma”. Isso significa dizer que os “produtos e serviços oferecidos e divulgados nas plataformas digitais são dependentes no senso de que são maleáveis, desenvolvidos para um determinado objetivo, porém adaptados de acordo com o *feedback* de usuários” (p. 4276). Esta realidade compromete a indústria midiática, já que a atenção se volta aos temas que têm maior chance de gerar engajamento, ficando de lado aqueles com menor adesão. Há ainda o fator das bolhas de público de cada rede social.

No caso do Twitter, Dagoula (2019) notou que há uma discussão centrada na elite presente, voltada principalmente à política. A característica desta rede em particular demonstra que mesmo aberta a todos, a plataforma dá voz a poucos. Os que se utilizam dela para se expressar fazem parte de um grupo seleto, perde-se, neste sentido, a pluralidade de opiniões.

A ideologia que vai ditando regras de como se deve viver e conviver em sociedade se tornou a práxis das redes sociais digitais. A emissão de opinião sobre todos os temas da vida cotidiana é vista como uma forma de arrebanhar seguidores, formando uma horda de apoiadores. Novamente, a busca é por engajamento, que proporciona a propagação de ideias. Todos estão preocupados, aparentemente, em mudar o mundo e não o interpretar. A formação da opinião migrou dos meios de comunicação de massa para as redes sociais. O consenso se transformou em meta, não há discussão de ideias, porque as redes primam pela aceitação (Rüdiger, 2016).

Uma das consequências visíveis é o impacto na produção de notícias. Antes do advento da internet, a decisão sobre a cobertura de um assunto pela mídia analógica passava pelos critérios de noticiabilidade: amplitude, frequência; relevância, conformidade, imprevisibilidade, continuidade, clareza, personificação ou significado, referência com pessoas de elite, assim como nações economicamente bem-posicionadas, composição e negatividade. Na sociedade da informação, o interesse do público e a capacidade de distribuição da notícia é parte inseparável do trabalho jornalístico (Harcup; O’neil, 2017).

Profissionais da mídia se relacionam com a audiência por meio de interação via redes sociais digitais e comentários das notícias publicadas. Os jornalistas também

fazem uso das métricas aferidas das publicações, que podem ser acompanhadas em tempo real, a partir do momento que são lançadas na internet. Perde-se de vista a lógica da produção jornalística e adapta-se a notícia à prática da rede social, que tem o objetivo de gerar cliques (Broersma; Eldridge II, 2019).

Em 2015, jornalistas do New York Times começaram a receber recomendação de produção de conteúdo sobre determinados tópicos, sobre os quais as pessoas buscavam informações. O serviço fazia parte de um aplicativo que fazia o rastreio dos interesses da audiência em mecanismos de buscas de plataformas digitais. O desenvolvimento destes aplicativos que monitoram cliques, compartilhamentos e *likes* é uma realidade do mercado da indústria cultural digital. Plataformas como Facebook, Twitter, Youtube e Academia.edu oferecem estatísticas detalhadas aos usuários sobre conteúdo e interação do público (Manovich, 2018).

A prática do jornalismo sofreu uma grande influência da organização da mídia em plataformas. Bossio (2017) sinaliza para a mudança de paradigmas profissionais relacionados à objetividade, aos processos de checagem de informação e ainda de autonomia profissional sobre o trabalho individual. No caso, a objetividade impedia que o jornalista levantasse bandeiras ideológicas em sua prática profissional, já os processos de checagem garantiam a veracidade da notícia postada e a autonomia do jornalista supunha que ele publicaria uma notícia porque o fato era de interesse público.

Porém, “as normas práticas do jornalismo fizeram uma transição em resposta às possibilidades sociais e tecnológicas, proporcionadas pelo aumento no uso de redes sociais” (Bossio, 2017, p. 24). Estas mudanças estão descritas no Quadro 2.

Quadro 2 – Mudanças nas práticas jornalísticas na era digital

Objetividade x Autenticidade		**Verificação x Transparência**		**Autonomia x Colaboração**	
Manter o distanciamento do fato, sem emitir opinião a respeito	Prática de auto expressão herdadas dos blogs	Verdade unitária de um evento, que pudesse ser apurada	Abertura do jornalista e da notícia para o escrutínio público	Seleção e priorização de notícias, em detrimento de outras	Participação pública e envolvimento da audiência com a notícia

Diferenciação da classe profissional para a prática amadora	Promoção de conteúdo compartilhável, identitário	Imparcialidade, levantamento de todos as partes história	Explica a forma de seleção de fontes ou de notícias	Escolha das fontes de informação e entrevistados	Utilização de material de testemunhas dos fatos
Servia como cláusula de barreira para profissionais incapazes de mantê-la	Oportunidade-de conexão social e atração de públicos para as notícias	Relato da verdade, com exatidão e precisão de interpretação	Publica-se *links* para as bases de checagem e entrevistas sem corte	Adoção de contexto e argumento para apresentação da notícia	Acomodação de opiniões e colaboração de públicos engajados
Princípio inviolável da ética profissional	Promoção de conteúdo por afinidade e não por autoridade	Ao determinar a verdade o jornalista se coloca como detentor da notícia	Abre-se a possibilidade de apontamentos de erros	Coloca o jornalista na posição do *"gatekeeper"* da notícia	Promove a construção coletiva em detrimento de uma visão única do fato

Fonte: elaborado pela autora com base em Bossio (2017)

Johnston e Wallace (2019) propõem alguns parâmetros que diferenciam os produtores de conteúdo dos jornalistas. Os profissionais da mídia são aqueles que trabalham com atividades editoriais de geração ou agregação de notícias, informações ou opiniões; estas divulgações devem ter um público-alvo; as publicações são periódicas; e o editor precisa responder a um código de ética. Jornalistas e empresas de mídia tiveram que seguir o curso da história e se atualizar às necessidades de um público e do ecossistema de produção que evoluiu com a internet, porém, a legislação não acompanhou.

Questões ligadas ao privilégio da imprensa, como manutenção do anonimato da fonte ou, então, de responsabilização pela difamação de alguém dependem do estabelecimento de quem é ou não profissional da área. Nos Estados Unidos, o assunto foi tema de debate desde 2009, quando teve início a discussão sobre a Lei de Livre Circulação da Informação, com apoio de 60 veículos de imprensa. A Lei foi aprovada em 2013, com alguns estados dando absoluta proteção, outros colocando algumas exceções e outros ainda, qualificações que estabelecem quando o privilégio pode ser evocado. A discussão também vem sendo feita em outros países como observaram Johnston e Wallace (2019), o entrave reside principalmente na definição de quem é ou não pertencente à imprensa profissional:

- no Canadá, jornalista foi definido como pessoa que tem sua principal atividade remunerada a contribuição para edição de informações e notícias, editoriais ou colunas para a mídia;
- na Nova Zelândia jornalista recebeu a definição de pessoa que na sua relação de trabalho recebe informações de uma fonte, na expectativa de que estas sejam publicadas, em um meio de notícias, que vai tornar os fatos públicos;
- na Austrália, em razão de motivos ligados à segurança nacional, depois de 11 de setembro, o indivíduo que publicar informações relacionadas à segurança nacional em redes sociais pode ser responsabilizado como qualquer outra pessoa, sem privilégios de jornalista.

No Brasil, o Marco Civil da Internet (Lei 12.965, 2014), em seu artigo 18º, tratou da não responsabilização do provedor de internet por conteúdo publicado, a não ser que seus administradores se recusem a retirar publicação em caso de acionamento judicial. A Lei 12.965 prevê a responsabilização por dano causado em publicação, mediante o artigo 5º da Constituição Federal, que trata dos deveres individuais e coletivos. O referido mecanismo legal institui o direito de resposta e a punição por calúnia e difamação. Já o artigo 220º da Constituição prevê a livre manifestação do pensamento e de divulgação de informações, sem restrição do poder público (Brasil, 1988).

A responsabilização da imprensa em caso de infração a direitos individuais ou questões relacionadas à segurança nacional entram em discussão em virtude de que na internet, a produção de conteúdo é matéria de domínio coletivo. No ecossistema desenvolvido pelas plataformas digitais a imprensa profissional, que se pauta por um código de ética e entende de suas responsabilidades junto ao público, passa a dividir espaço com produtores de conteúdo. Assunto que será discutido na próxima seção.

2.4 Exploração da criação de conteúdo pelos usuários

As plataformas agregam valor aos seus usuários em três aspectos, de forma interna, externa ou numa combinação entre as duas anteriores. Na geração de valor interno, a própria plataforma fornece produtos ou serviços aos usuários; na externa, ela agrega valor com produtos e serviços de terceiros, como desenvolvedores de aplicativos, por exemplo; na terceira forma agrega valor utilizando tanto material próprio, como agregado. Quanto maior é a agregação externa, menor é o gasto com

funcionários, já que estas plataformas se valem da lógica de transformar em usuários os seus complementadores (Parker; Petropoulos; Van Alstyne, 2020).

O fenômeno da plataformização, de acordo com Burgess (2021), trouxe uma nova forma de tratar conteúdo, com um ecossistema que proporciona conexões, mineração de dados e interfaces com outros websites. A lógica de alcançar popularidade, pelas conexões, é a principal meta de criadores de conteúdo como vídeos, músicas e *realities*, que buscam, por meio de suas métricas, atestar sua relevância na rede. O criador de conteúdo busca o posto de referência em seu tema de produção, para ser alcançado ao patamar de *influencer* digital. Ele vai depender, porém, de como a plataforma faz a leitura e estabelece o algoritmo de suas métricas, o que não é um mecanismo claro e acessível de compreensão.

Manovich (2018) pontua que a análise de interação interpessoal ou grupal não era uma realidade possível na produção midiática do século passado. Já na sociedade dominada pelas redes sociais, a leitura de dados proporciona o detalhamento destas interações. Faz parte do ecossistema das plataformas digitais a recomendação de consumo de bens culturais, via direcionamento algorítmico. Nesta fase, a distribuição do conteúdo midiático encontra seu máximo resultado, já que o algoritmo é desenvolvido neste sentido.

Há aplicativos que recomendam a melhor hora para fazer *posts* nas redes sociais, dependendo do perfil de seus usuários. Depois do conteúdo postado, é possível dar início a uma campanha de distribuição do *post* baseado em idade, gênero, localização e interesses. As ferramentas de anúncio tornam possível, inclusive, buscar por usuários semelhantes àqueles que já estão na base de seguidores. O investimento massivo de plataformas digitais em inteligência artificial torna possível a customização de anúncios, indicando direcionamento de público-alvo especificamente definido (Manovich, 2018).

Um estudo feito com consumidores chineses demonstrou como as plataformas digitais têm se aproveitado, por exemplo, das transmissões ao vivo de celebridades para a venda massiva de produtos. A pesquisa apontou como o conteúdo de *influencers* digitais, que fazem propaganda indireta de produtos, ajuda as empresas a escalarem globalmente sua comercialização. Estes *influencers,* que se apoiam na criação de conteúdo digital, têm nichos extremamente marcados por um público-alvo nichado. Tudo o que produzem relacionado ao assunto que dominam, como maquiagem, *anime*, *games*, tem audiência cativa (Park; Lin, 2020).

Esta ação é conhecida como marketing de influência, que nasceu a partir da cultura dos blogs, a partir dos anos 2000. Os blogueiros eram, em sua maioria, jornalistas que escreviam sobre um assunto específico, como resenha de livros, crítica de cinema, política, economia e esporte. Jornalistas geralmente faziam este trabalho como *hobby*. A diversidade da blogosfera foi se multiplicando e novos blogueiros entraram neste universo, sem formação profissional na comunicação. Munidos de credibilidade e prestígio na rede, estes profissionais começaram a emprestar suas imagens para campanhas publicitárias (Karhawi, 2021).

A prática, utilizada no passado, se transformou com a entrada das plataformas digitais de relacionamento social no mercado. Artistas, atletas, gente que ficou famosa pela participação em algum *reality show,* e mesmo anônimos que construíram sua identidade e audiência nas plataformas, passaram a ser as novas caras de produtos e serviços na rede social. Os *influencers* estimulam o comportamento consumidor da audiência na internet. Em algumas situações, os *posts* feitos nas redes sociais são identificados como *publipost*, ou seja, conteúdo pago. Porém, nem sempre o pagamento pela veiculação de uma propaganda é mencionado (Park; Lin, 2020).

O entretenimento é apenas uma das formas de exploração da criação de conteúdo pelas plataformas de mídias sociais. No caso dos *influencers*, seus conteúdos têm métricas aferidas e é por conta deste engajamento comprovado que eles conseguem contratos e recebem pelo produto ou serviço divulgado. Mas muitos, em início de carreira, apenas compartilham com a audiência os “recebidos” de empresas que têm relação com o conteúdo que produzem. A monetização de conteúdo postado é, na maior parte das vezes, estabelecida pelo engajamento com a audiência, determinada pela leitura de dados. É o que vem sendo chamado de *data-driven model business* (DDMB), traduzindo, modelo de negócio moldado pelos dados (Isabelle; *et al.*, 2020).

Segundo Isabelle *et al.* (2020), este modelo de negócio é a base das plataformas digitais, que se apresentam como ambientes multifacetados para diversos setores, desde o comércio varejista, à indústria editorial, produtos financeiros e até seguradoras. A análise dos dados de navegação dos usuários tem como objetivos: “aumento de receita, redução de custos, retenção de clientes valiosos, previsão de comportamento consumidor, otimização da experiência de compra e ofertas direcionadas de produtos anteriormente pesquisados” (p. 04). Para atrair e manter clientes nas plataformas, estas precisam ter conteúdo renovável constantemente.

Além da produção, as plataformas dominam também a distribuição dos bens digitais e, portanto, dão maior ou menor importância aos conteúdos de acordo com seus interesses econômicos e ideológicos. Complementadores perdem criatividade, espontaneidade e são convertidos em desenvolvedores de conteúdos que obedecem aos algoritmos de monetização, moldando produtos culturais às métricas de distribuição da plataforma para a qual desenvolvem produtos baseados em interface de interação com o usuário final (Nieborg, Poell, 2018, p. 6).

> As relações de poder entre operadores de plataforma, usuários finais e complementadores são extremamente voláteis e inerentemente assimétricas, uma vez que os operadores são totalmente responsáveis pelo desenvolvimento tecnoeconômico de uma plataforma.

Filgueiras e Antunes (2020) vão resumir em três paradigmas o trabalho em plataformas digitais: a negação do assalariamento, sem contratos empregatícios; uso de um mecanismo que torna o empregado um cliente da plataforma, camuflando a figura de empregadora; e, apesar da tecnologia viabilizar o controle da atividade laboral, inclusive de forma remota, isso não ocorre. As plataformas têm, em sua maioria, precarizado as relações de trabalho, num sistema que individualiza a prestação do serviço, evitando a organização de classes.

As plataformas digitais criaram um ambiente inovador e criativo, dando origem a um ecossistema disruptivo, isso é inegável, de acordo com Ribeiro e Hebster (2020). Porém, este ecossistema é colocado em risco, quando se observa a forma como os direitos à propriedade intelectual vêm sendo tratados. Produtores de conteúdo têm sua atividade laboral apropriada pelas plataformas, com formulação de recompensa produtiva nebulosa, feita por meio de algoritmo de dados, medidos pela interação da audiência, sem que eles tenham qualquer controle sobre os padrões de remuneração.

Visto de perto, o trabalho nas plataformas tem acentuado as desigualdades sociais que há muito se perpetuam pelo mundo. Na Europa e Estados Unidos trabalhos digitais são feitos por meio de contratos de *freelancers*. A prática foi intensificada a partir da crise econômica de 2008. No Brasil e demais países da América Latina ofícios informais sempre fizeram parte da lógica de mercado. As plataformas costumam delegar serviços mais mecanizados e simplificados em moedas mais baratas. Atividades mais complexas, com valor agregado maior, são destinadas a trabalhadores de países com maior nível de formação acadêmica. Desta

forma, Grohmann (2020) classifica o trabalho em plataformas como detalhado no Quadro 3.

Quadro 3 – Classificação do trabalho em plataformas

TIPOS DE TRABALHO	EXIGÊNCIAS	EXEMPLOS
Plataformas de trabalho por georreferenciamento	Precisam do trabalhador em um determinado tempo e espaço para realizar uma atividade numa localidade	iFood, Rappi, Uber, 99Taxi, Deliveroo, etc.
Plataformas de microtrabalho ou *crowdwork*	Trabalhadores “treinam” os dados que depois serão utilizados como inteligência artificial	Amazon Mechanical Turk, PiniOn, MicroWorkers
Plataformas *freelance*, de *cloudwork* ou macrotrabalho	Trabalhadores executam microtarefas previamente contratadas que vão desde a pintura até passeio de animais	GetNinjas, WeDoLogos, Freelancer, iPrestador, 99Designs

Fonte: elaborada pela autora com base em Grohmann (2020, p. 113)

Muitos autores classificam estas atividades laborais como uberização do trabalho. Grohmann (2020) prefere o termo plataformização do trabalho. A metáfora da Uber, na visão do autor, simplifica o tema e não compreende a complexidade de trabalhos mediados por plataformas. Entre eles todo o ecossistema necessário para coletar, classificar e aferir valor aos dados extraídos a partir da interação de usuários e produtores de conteúdo. Além disso, há uma lógica implícita de empreendedorismo digital que suprime direitos trabalhistas, sem eliminar relações de subordinação, dando flexibilidade apenas ao empregador para impor entrega sem especificação de horas para conclusão das tarefas e condições estruturais para exercício da atividade.

Uma das formas de trabalho comuns no sistema de plataformas é o lançamento de desafios. Estes são geralmente problemas para os quais a empresa não encontra solução. No mundo todo, trabalhadores podem apresentar projetos de resolução da questão. O vencedor recebe um prêmio, geralmente em dinheiro, enquanto os demais que gastaram tempo e energia em uma proposta ficam de fora da remuneração. É a terceirização da área de pesquisa da empresa, que não precisa manter um local e uma equipe na busca da solução de problemas inerentes ao setor. É um sistema colaborativo de trabalho, sem pagamento e segurança trabalhista (Franco; Ferraz, 2019).

Filgueiras e Antunes (2020) resumem em três os principais conflitos das plataformas digitais e as relações trabalhistas: as regras de assalariamento são mascaradas, sob a base de maior autonomia produtiva. Desta forma, desaparece o papel de empregador; e, por fim, a economia digital despersonaliza o trabalhador, envolto no sistema da rede. Um exemplo desta realidade são os entregadores do Ifood, que estão inscritos no aplicativo e prestam serviço de entrega a diversos restaurantes também cadastrados. Nenhum dos envolvidos é empregado do outro, ainda assim prestam serviço entre si.

Sob a égide do tecnológico, contemporâneo e disruptivo, os oligopólios das plataformas se apropriam do valor gerado por trabalhadores como motoristas, entregadores de comida, produtores de vídeos, professores e autores de publicações online. Ninguém mais governa a si mesmo neste ambiente ubíquo, em que a plataforma a todos vê e controla. Como mercados multilaterais, as plataformas vão ficando no centro do poder. Tudo isso é amparado por um sistema de extração e expropriação de dados de seus usuários, que desconhecem a extensão da invasão a que estão expostos, este é o tema do próximo ponto.

2.5 Segurança e privacidade do usuário

Um estudo feito pelo Office of the Australian Information Commissioner demonstrou que 58% dos usuários da internet admitem não saber o que é feito com seus dados pessoais quando navegam na rede e 49% informaram que não têm ideia de como se proteger devido à falta de tempo para pesquisar sobre a complexidade do (Competition, 2020). A venda de dados pessoais de 87 milhões de usuários do Facebook, em 2016 para a Cambridge Analytica, que minerou, modulou e utilizou os dados para influenciar eleitores estadunidenses, no pLeito à presidência dos Estados Unidos, demonstra o valor dos dados e a falta de disposição das plataformas em protegerem seus usuários (Flew, 2018).

A informação veio à tona em 2016, porém, a primeira campanha de Barack Obama ao governo do país, em 2008, já utilizou, de forma tímida, as redes sociais. Era o começo das plataformas de relacionamento virtual e uma equipe jovem compartilhava *posts* na rede. Em 2012, quando a coleta já estava mais avançada e poucas eram as barreiras, a Cambridge Analytica participou da campanha para a reeleição de Obama, com a ajuda de uma antiga funcionária da primeira investida do

presidente Obama à Casa Branca, Brittanny Kaiser. A entrada da empresa na estratégia do candidato previa a utilização de dados de 270 mil usuários de Facebook e seus amigos. A ação ajudou Obama a vencer a disputa em 26 estados mais o Distrito de Columbia, deixando Mitt Rommey em segundo com 24 estados na somatória final[13].

De acordo com Flew (2018), na campanha de 2016, mensagens moduladas para usuários faziam com que *posts* de um mesmo candidato, sobre um único assunto, tivessem 50 versões diferentes, customizadas para perfis diversos de usuários. A exposição do modo de ação da Cambridge Analytica levou a empresa à falência. O episódio demonstrou como empresas de propaganda e plataformas de mídias sociais trabalhavam com as informações dos usuários. Há ainda um outro problema, a concentração de mercado no setor. Google e Facebook são responsáveis por 70% de todo o tráfego de internet. Quando o assunto é anúncio, Google congrega 90% da fatia de mercado em plataformas de buscas e Facebook com 80% do interesse nas de redes sociais. No mercado editorial, Amazon detém 75% das vendas de *e-books*.

Um dos riscos de um mercado digital global sem regulação é a exposição da privacidade dos usuários. Falta clareza sobre a forma como as informações são extraídas, classificadas e utilizadas. Um exemplo desta realidade é a apropriação pela indústria midiática de atividades prosaicas como tomar água, fazer dieta e exercícios, que têm sido exploradas por uma infinidade de aplicativos. A inteligência artificial lembra os usuários dos *app*s qual a hora de se hidratar, quantas calorias comeu ao longo do dia ou então quantos passos ainda faltam para atingir a meta de movimento mínimo para a perda de peso. Couldry e Mejias (2019) vão chamar esta prática das plataformas de colonização por dados, numa forma distinta de exercício de poder.

É difícil encontrar algum negócio que seja independente da classificação social digital. Mesmo produtos analógicos, como os imóveis, precisam do auxílio da tecnologia para atingir seu público-alvo, em direcionamento de vendas. “A qualidade de vida das pessoas com certeza foi impactada pela coleta de dados, para uso futuro na obtenção de lucro, o que era inimaginável duas décadas atrás” (Couldry, Mejias, 2019, p. XV). Com uma exploração em larga escala, a mineração dos dados faz a

---

13 *Former Cambridge Analytica exec says she wants lies to stop.* Disponível em: https://www.theguardian.com/uk-news/2018/mar/23/former-cambridge-analytica-executive-brittany-kaiser-wants-to-stop-lies Acessado em 29/08/2021.

seleção natural dos consumidores, posicionando-os, por meio do algoritmo, nas categorias de fracos ou fortes no potencial de compra.

É possível notar que o uso dos dados para melhorar a experiência de *e-commerce* evoluiu para outros fins como: política, saúde pública, controle social e aplicação da Lei. “A relação com o usuário é para retê-lo na plataforma, saber quais são aqueles mais influenciáveis, para os conduzir na identificação com marcas de toda sorte de produtos ou serviços nas redes sociais” (Mansell; Steinmuller, 2020, p. 06). O sistema de coleta de dados para direcionamento de usuários propicia à plataforma um aspecto de governança que retira do indivíduo seu real direito de escolha.

O acúmulo de influência econômica, social e política das plataformas digitais chamou a atenção dos governos ao redor do mundo. Na construção deste poder, as plataformas fizeram uso de ferramentas como: destruição de competidores menores, disseminação de desinformação, permissão de manipulação política e invasão da vida privada dos usuários. Estes comportamentos geraram insatisfação e despertaram a necessidade de intervenção de firmas especializadas em governança corporativa, coalizão de segmentos econômicos e de governos, na busca por normas de regulação (Cusumano; Gawer; Yoffie, 2021).

Em 2016, a União Europeia deu início a uma série de ações na tentativa de regular questões referentes aos problemas encontrados nas plataformas digitais. Ações antitruste contra a Google foram feitas em 2016 e 2017. Nos Estados Unidos, as ações começaram em 2020, contra Facebook e Google. A invasão do Capitólio nos Estados Unidos, no início de 2021, acendeu mais um alerta. “Ironicamente, enquanto a reputação de algumas plataformas digitais caía, suas revisões e lucros aumentavam, especialmente durante a pandemia de Covid-19, que fez com que vários negócios migrassem para a internet” (Cusumano; Gawer; Yoffie, 2021, p. 1261).

Ribeiro-Navarrete, Saura e Palácios-Marqués (2021) apontam que justamente a pandemia de Covid-19 implicou em uma maior vigilância, por parte das plataformas, ao comportamento do usuário. Utilizando principalmente dados extraídos dos consumidores de conteúdo online via *smartphones,* que são maioria. As plataformas poderiam informar por georreferenciamento a localização dos aparelhos em períodos de *lockdown*. Além disso, foram identificados ao menos 13 aplicativos, oferecidos aos usuários de forma gratuita, que verificavam, por exemplo, o contato do usuário com pessoas infectadas. Os apps não só analisavam a movimentação física do internauta, mas todo o seu consumo e produção de conteúdo.

Todas as informações foram compartilhadas com terceiros, a pretexto de detecção de possíveis indivíduos contaminados ou mais propensos a contraírem a Covid-19. Os dados foram divididos não só com governos, mas também com empresas particulares, que podiam destinar estas informações para fins além da preocupação sanitária. Os termos de uso dos *apps*, em sua maioria, não previam intervalo temporal de armazenamento das informações, identificação de usuário, destinação dos dados coletados e formas de utilização, numa clara exposição da privacidade dos indivíduos (Ribeiro-Navarrete; Saura; Palácios-Marqués, 2021).

De acordo com Kuenzler (2022), há duas formas de tratar as questões relacionadas à privacidade dos usuários de plataformas digitais. A primeira reside no indivíduo como usuário da plataforma, que compreende uma relação de consumo. Neste caso, a proteção aos dados pessoais poderia ser uma preocupação quando da escolha da plataforma de rede social à qual o consumidor decidisse aderir. O problema, porém, reside na concentração de mercado, que reduz as opções. A segunda questão se volta à relação de produtor de conteúdo, que tem com a plataforma uma relação de prestador de serviço. A plataforma depende da produção de terceiros para agregar novos usuários. Neste sentido, associações de produtores poderiam exercer poder em demandas relacionadas à privacidade dos dados coletados.

Na Alemanha, uma investigação do Federal Cartel Office (FCO) constatou que o Facebook obrigava os usuários a concordarem com termos de uso nos quais permitiam a mineração de dados fornecidos na plataforma de relacionamento social, em sites e aplicativos parceiros. O FCO apontou que ao usuário não era oferecida uma opção, caso não concordasse com esta regra. A personalização de navegação é uma ação possível, porém, não era oferecida aos usuários que quisessem restringir acesso de seus dados a terceiros. Quem não concordasse com os termos de uso, na íntegra, não poderiam aderir à plataforma. A falta de competição neste mercado deixava o usuário discordante fora da plataforma que concentra a discussão pública de ideias no ciberespaço (Kuenzler, 2022).

No ponto 3.5 serão tratadas as iniciativas de movimentos populares e sociedade civil organizada para a criação de parâmetros de regulação das plataformas de mídias sociais. No próximo capítulo serão tratadas as bases necessárias para estabelecimento de parâmetros de regulação de plataformas digitais, de maneira que seja mantida a liberdade de expressão, privacidade do usuário e segurança na rede.

3 – BASES DE ESTRUTURAÇÃO PARA A REGULAÇÃO DAS PLATAFORMAS

Uma relação de confiança no ciberespaço é estabelecida quando o compartilhamento de informações é feito a partir de regras transparentes, prestação de contas, garantia de privacidade e efetiva segurança do usuário. Estas seriam as bases nas quais a regulação de plataformas digitais deveria se apoiar. A identificação dos riscos de exposição do usuário devem ser uma preocupação constante, tanto de empresas particulares como de governos. A prática de compartilhamento de dados de usuários com terceiros é frequente em ambas as formas de oferta de serviço, tanto privados, como governamentais.

As plataformas digitais, propriedades de empresas transnacionais, têm sido avaliadas por organismos internacionais. Estas empresas são opacas na oferta de explicações sobre as formas de coleta, processamento, estocagem e compartilhamento das informações particulares de seus usuários. A prática comum é de utilização dos dados para aferição de lucro, seja por direcionamento de anúncios ou então pela venda das informações para confecção de produtos e até novas plataformas.

O serviço público, ofertado aos cidadãos via plataformas de *e-govermment* que se multiplicaram ao longo dos últimos anos*,* também falha em questões relacionadas à transparência na oferta de um ambiente seguro e igualitário. No caso dos governos digitais, a população resiste à utilização dos serviços devido à falta de confiança nos sistemas de informação estatal e até mesmo de eficiência nas soluções ofertadas no ciberespaço.

Neste capítulo a seção 3.1 traz os princípios para a regulação, que usam como base questões fundamentais para nações, não apenas objetivos; no ponto 3.2 são tratadas as diferenças e semelhanças de processos de autorregulação, que partem das plataformas, da regulação dos legisladores, em forma de Leis e de iniciativas conjuntas (corregulação) entre público, privado e sociedade civil organizada; a seção 3.3 trata dos principais entraves na transparência da prática de atividade das plataformas digitais comerciais. Na seção 3.4 é apresentado um dos principais problemas das plataformas: a falta de transparência na oferta de serviços online. Já na seção 3.5 busca-se apresentar alguns exemplos de ações fiscalizatórias por parte da sociedade civil às plataformas e, por fim, na seção 3.6 são elencados alguns

parâmetros que podem ser norteadores para o processo de construção de um arcabouço legal de regulação nas sociedades democráticas.

3.1 Princípios para a regulação

Quando legisladores e agências reguladoras consideram princípios para a confecção de normas para as plataformas digitais precisam levar em consideração pontos que visem reduzir riscos e fortalecer atividades benéficas à sociedade como um todo. Os princípios são mais importantes que os objetivos na tarefa de regulação. É complicado alinhar objetivos entre diferentes culturas, economias e tradições nacionais. Já os princípios podem ser compartilhados entre nações que comungam dos mesmos valores. Nações democráticas, por exemplo, compartilham de uma série de crenças filosóficas fundamentais, como direitos individuais, senso de comunidade, participação igualitária dos cidadãos e responsabilização (Picard; Pickard, 2017).

Os princípios podem ser divididos em sete frentes de ação. O primeiro diz respeito à satisfação integral do direito à comunicação e informação dos cidadãos. Em segundo lugar, a regulação deve garantir o uso público dos meios de comunicação. Como terceira exigência, emprega-se a necessidade de contemplar diferentes pontos de vista na esfera pública. O quarto princípio reside na proteção da sociedade. Em quinto lugar está a necessidade de transparência do processo de responsabilização de quem causar qualquer tipo de dano. Como sexta premissa, estabelece-se a busca pelo desenvolvimento econômico. Com vistas, em último aspecto, a resultados políticos equitativos e eficazes (Picard; Pickard, 2017).

A regulação serve como um ato de colocar em perspectiva as necessidades públicas, interesses governamentais e demandas corporativas. Apesar de parecer igualitária, a infraestrutura da plataforma existe para servir a seus próprios interesses, defendendo ideologias próprias, por meio de normas de utilização opacas, que ao invés de empoderar o usuário o coloca numa posição inferior a quem comanda a plataforma. Neste intuito defende-se que a regulação não deve ficar a cargo das plataformas que acabam interferindo não apenas na esfera privada, mas na pública também. Outro ponto de questionamento reside no fato de os EUA dominarem a comunicação pública mundial, já que a maior parte das plataformas digitais está baseada em solo estadunidense (Bizberge; Mastrini; Gómez, 2023).

O modelo estadunidense, desde a década de 1990 tem sido de autoridade descentralizada, auto governança das plataformas e dependência de concorrência de mercado, em detrimento de regulação estatal. Um problema se instala porque as exigências com relação à legislação estadunidense é uma, enquanto ao redor do globo as plataformas encontram realidades diferentes. O Facebook, por exemplo, mantém um time focado na moderação de conteúdo na Europa, devido à legislação da UE, que tem mecanismos legais para o tratamento de conteúdo terrorista; referente a abuso sexual e aliciamento de menores; e, com foco na segregação de minorias. Na era da internet a maior dificuldade para as nações democráticas é criar um *framework* de Leis que contemple tanto as empresas de mídia tradicional que compreendem TV, rádio e jornais, como as de mídias sociais (Flew; Martin; Suzor, 2019).

Os maiores desafios da regulação das plataformas digitais residem em quatro dimensões: o ritmo, que nem sempre acompanha a evolução das infraestruturas tecnológicas; a projeção de normas que sejam adequadas a condutas específicas, que não são englobadas por regras genéricas; os desafios ligados à aplicação do regramento e fiscalização de seu cumprimento; e, as questões transfronteiriças (Malyshev; Kauffmann, 2019)

Com esta preocupação em mente, os governos de União Europeia, Austrália, Reino Unido e Canadá vêm discutindo formas de regular as plataformas digitais. Assim como a OCDE vem buscando uma forma de taxar globalmente as *big techs* em até 15%, criando fundos para execução de políticas públicas no setor. Um dos maiores pontos de alerta está na moderação de conteúdo e as implicações sobre a liberdade de expressão, base da Primeira Emenda da Constituição estadunidense. A tarefa de regular discurso é delicada e exige do legislador um cuidado extremo na retirada de conteúdo prejudicial, ao mesmo tempo que se mantém a exposição de posicionamentos controversos. Além disso, é preciso combater conteúdo perigoso, porém, mantendo-se espaço para o debate de ideias (Bizberge; Mastrini; Gómez, 2023).

> Mas a maioria dessas iniciativas legais configura soluções que são desproporcionais e ampliam o risco de violações ao direito à livre expressão, uma vez que atribuem responsabilidades e obrigações que tornam as plataformas juízes ou polícias privadas sobre os conteúdos de terceiros que podem circular na Internet (Intervozes, 2020).

As plataformas estadunidenses legitimaram a visão liberal e impuseram esta realidade aos demais países do globo por meio de suas normas autorregulatórias. Alguns estudiosos apontam que uma alternativa seria a regulação das plataformas digitais como serviços de utilidade pública; outros propõem a regulação como se fossem empresas de mídia; e, há ainda quem acredite que é preciso olhar a infraestrutura como um todo, observando fluxo de dados, relação de propriedade, inter-relações técnicas e controle organizacional. Mas ao final da discussão sobre o modelo de regulação sempre sobra o questionamento de quem faria a fiscalização das normas impostas. Além do que já está posto, que é a criação de uma regulação estatal, novos atores entraram no processo como entidades supranacionais, oligopólios globais e sociedade civil organizada (Bizberge; Mastrini; Gómez, 2023).

Na tentativa de encontrar novas soluções, um grupo de acadêmicos propôs uma regulação progressiva para tipos específicos de plataformas. Primeiro estariam inclusas apenas plataformas de mídias sociais, motores de busca e de distribuição de vídeos. A proposta prevê uma regulação progressiva, conforme o domínio de tal plataforma na distribuição de conteúdo. Quanto maior o domínio de mercado, maior o controle. O mecanismo incluiria autorregulação, corregulação e regulação pública (Intervozes, 2020).

As normas tratariam de limites para a moderação de conteúdo, compatíveis com parâmetros internacionais de direitos humanos, levando em consideração a proteção de minorias e grupos vulneráveis; também com mecanismos de defesa contra governos autoritários, retirando delas a responsabilização pelo conteúdo de terceiros, ou vigilância do material postado. A proposta deveria trazer ainda instrumentos antimonopólio, aumentando o número de plataformas enfrentando o cenário de concentração e aumentando a concorrência. A construção deste arcabouço legal passaria pela transparência, garantias processuais e limites aos termos de serviço (Intervozes, 2020).

Ruediger *et al.* (2022) reforça que o modelo de autorregulação data do princípio da internet, ainda na década de 1990, com a Declaração de Independência do Ciberespaço. A regulação era identificada como supressora de liberdade de expressão, porém, no princípio a lógica da rede era descentralizada, com vários atores disseminando conteúdo. Na realidade contemporânea as plataformas estão cada vez mais centralizadas e formam os oligopólios transnacionais.

A dependência da população da América Latina a estas plataformas torna o tema urgente. Em países como México, Argentina e Peru, 60% dos entrevistados da pesquisa Digital News Report 2022, da Reuters, admitiram que usam redes sociais como fonte de informação primária. Como a maior parte das nações, na América Latina discute-se majoritariamente a moderação do conteúdo digital e fundos de auxílio à mídia tradicional, porém, o que se percebe é que mesmo com taxação, os recursos não têm servido para pluralização cultural e podem intensificar ainda mais a concentração de monopólios de comunicação locais, que recebem maior parcela do dinheiro arrecadado, invisibilizando ainda mais canais independentes (Bizberge; Mastrini; Gómez, 2023).

Na Europa, a Comissão Europeia convocou as empresas de tecnologia para criarem o Code of Practice on Disinformation, em 2018. Um dos focos do documento tratava da elaboração de normas sobre anúncios de campanhas eleitorais no território europeu. A principal alegação da UE para permitir que as plataformas fizessem as suas próprias normas neste quesito residiam no fato de que o setor teria a expertise para criar as regras e que não haveria tempo hábil, até as eleições da Comissão Europeia, para que o processo legislativo fosse concluído com Leis que englobassem conteúdo de campanha (Wolfs; Veldhuis, 2023).

Uma das premissas pensadas para a utilização de anúncios online, que era a divulgação em todo o território europeu do processo decisório nas eleições da Comissão Europeia, foi contrariada pelas normas autorregulatórias. O Facebook, por exemplo, restringiu os anúncios apenas dentro dos países de onde haviam sido originados. Como a maioria dos partidos mantinha sede em Bruxelas, as campanhas ficaram restritas à Bélgica. Com isso, a meta de ampliar a visibilidade das eleições da Comissão e do Parlamento Europeu ficaram restritas e impediram que o processo decisório do território comum saísse do segundo plano. Nos Estados-Membros as eleições internas estão em primeiro plano para seus cidadãos (Wolfs; Veldhuis, 2023).

O exemplo demonstra que a discussão sobre regulação deve ser ampliada e encampada por mais atores. Os projetos em discussão falham em pouco tratar sobre transparência e responsabilização das plataformas. A Organização dos Estados Americanos (OEA) vem trabalhando numa proposta com parâmetros de garantia da proteção de direitos humanos e diversidade de ideias, com foco em três áreas: moderação de conteúdo, literacia digital e debate público. A Unesco também desenvolveu um guia que abarca cinco princípios para a regulação das plataformas:

obrigação das plataformas no respeito aos direitos humanos na moderação de conteúdo; transparência na elaboração de termos dos serviços, moderação de conteúdo, atendimento a reclamações, e, anúncios; investimento em literacia digital para usuário, principalmente crianças e adolescentes; responsabilização por uso indevido de atividade algorítmica; e, combate à violência de gênero na rede (Bizberge; Mastrini; Gómez, 2023). Na próxima seção serão detalhados os modelos de regulação, autorregulação e corregulação,

3.2 Regulação, autorregulação e corregulação, diferenças e semelhanças

O Brasil foi um dos primeiros países a colocar em prática uma Lei, que previa mecanismos regulatórios para as plataformas digitais. O Marco Civil da Internet (Lei 12.965, 2014), de 2014, trouxe a base do regramento para comportamentos e negociações online. No ano de 2018, o Brasil voltou a discutir mecanismos regulatórios com a Lei Geral de Proteção de Dados, a LGPD (Lei nº 13.709/2018). Em 2020, o Projeto de Lei 2.630, apresentado pelo então senador Alessandro Vieira (CIDADANIA – SE), conhecido como PL das Fake News, reacendeu o debate (Ruediger *et al.*, 2022).

O modelo europeu de regulação teve seu primeiro processo legislativo finalizado em 2016, com a entrada em vigor do General Data Protection Regulation (GDPR). Já em 2022, duas novas Leis fizeram o detalhamento dos mecanismos regulatórios para diferentes âmbitos das plataformas digitais: Lei dos Serviços Digitais que responsabiliza as plataformas por disseminação de conteúdo ilegal e por riscos aos usuários; e, o Ato de Mercados Digitais, que tem um viés mais econômico, tratando de questões como promoção de inovação e competitividade no ambiente digital. Nos EUA o debate segue dividido entre concorrência, privacidade e desinformação (Ruediger *et al.*, 2022).

De acordo com Brega (2023), o modelo empregado pelo Brasil foi o de responsabilidade subjetiva das plataformas com relação a conteúdo postado por terceiros. Neste sentido, a plataforma não tem o dever de monitorar previamente o conteúdo dos usuários, funcionando apenas como intermediária da informação. Contudo, responde solidária e subjetivamente pelo conteúdo, caso se negue a atender uma determinação judicial sobre remoção do material. Para que a justiça decida é preciso haver uma notificação e, depois da decisão judicial, uma comunicação ao

usuário sobre a remoção, com abertura de espaço para o contraditório e a ampla defesa.

A responsabilização no Brasil versa sobre a omissão das plataformas no cumprimento de determinação judicial. O regramento não trata sobre a ação da plataforma, que por meio de seus mecanismos de autorregulação aplica remoção de conteúdo e até de perfis, segundo seu próprio entendimento de adequação às normas da comunidade. O risco que se observa é de que utilizando normas de autorregulação, as plataformas priorizem conteúdo de acordo com sua visão ideológica, marginalizando grupos contrários, intensificando a criação de bolhas e filtros de comunidades online (Brega, 2023).

Napolitano e Ranzani (2021), com base na literatura, sugerem a autorregulação regulada das plataformas digitais, segundo quatro fundamentos: 1) a participação de um órgão regulatório, que pode ser um comitê, uma agência reguladora, com representatividade diversa e mandato temporário; 2) a instituição de manuais de conformidade para elaboração das normas autorregulatórias das plataformas, com ratificação do órgão regulador, e, ainda a formulação de relatórios periódicos de transparência de dados; 3) proporcionalidade de regulação dependendo do tamanho da plataforma digital, com estabelecimento de condições mínimas de operação das plataformas; e 4) estabelecimento de limites negativos, para impedir que direitos fundamentais sejam usurpados.

A Network Enforcement Act (NetzDG), lei alemã instituída em 2017, de combate a discurso de ódio nas redes sociais, é citada como um dos exemplos de autorregulação regulada das redes sociais. A lei alemã tipifica os crimes praticados por meio de compartilhamento de conteúdo nas redes sociais. O instrumento trouxe para o mundo online a responsabilização que é presente no mundo físico. Napolitano e Ranzani (2021) entendem que a autorregulação regulada “pode ser vista como subsídio e anteparo à formação de novos marcos regulatórios, de novas agências reguladoras e de manuais internos de conformidade” (p.196).

Outra iniciativa feita por pesquisadores da América Latina apresentou uma proposta que elencou padrões para uma regulação que respeitassem parâmetros democráticos para as grandes plataformas que compartilham conteúdo. Os marcos regulatórios propostos incluem limites da regulação, como deveriam ser feitos os termos de serviços das plataformas, pontos referentes à transparência, devido processo legal na moderação de conteúdo, com perspectivas referentes ao direito de

defesa do usuário, assim como prestação de contas por parte das plataformas e mecanismos referentes à corregulação que incluem a autorregulação e o poder regulatório estatal (Pallero *et al.*, 2020).

A proposta dos pesquisadores latino-americanos prevê que a base regulatória precisa respeitar a liberdade de expressão online, que é parte integrante dos direitos fundamentais de qualquer pessoa, assegurado pela ONU. Os termos de serviços deveriam ser documentos obrigatórios de todas as plataformas, escritos de forma clara, objetiva, com linguagem acessível, que dessem condições ao usuário de compreender sob que condições ele poderia ter seu contrato rescindido. Além disso, os direitos autorais deveriam ser respeitados, porém, sem infringir o direito à crítica, denúncia ou fins educativos determinados, como apontam Pallero *et al.* (2020).

Os mecanismos de verificação em *upload,* frequentemente utilizados por Youtube, Facebook, Instagram e Twitter, são considerados censura prévia. A curadoria de conteúdo também deveria ter ordenamento claro e objetivo para que o usuário compreendesse em que condições poderia ter alcance e distribuição reduzidos ou material editado pelas plataformas. Em adição, conteúdo só poderia ser proibido em caso de ser manifestamente ilegal, propaganda em favor de guerra, apologia ao ódio nacional, racial ou religioso. E ainda, o conteúdo poderia ser restrito a grupos vulneráveis de acordo com o tema, no caso de crianças e adolescentes. Também deveria ser oferecida aos usuários a possibilidade de restringir visualização de acordo com temas pré-determinados (Pallero, *et al.*, 2020).

Para que o processo de moderação de conteúdo ocorresse segundo padrões democráticos, a proposta de Pallero *et al.* (2020) prevê a transparência referentes às informações tanto da parte das plataformas, quanto da do usuário. A preocupação se dá principalmente por conta da remoção de conteúdo ou até mesmo de contas, sem que o usuário saiba o que deu origem a tal ação. Há um cuidado previsto no devido processo legal, com espaço para notificação antecipada, ampla defesa e contraditório, com uma sinalização para juízo adequado na solução de conflito entre as partes.

A proposta retira das mãos das plataformas, na autorregulação, o poder absoluto e unilateral por causa da oferta dita gratuita dos serviços. Obrigando as empresas a consultarem o usuário quando da mudança de pactuação, com concordância do consumidor, corregulação. Neste sentido, um órgão público independente poderia ser instituído como fiscalizador do cumprimento das normas, com poder de emissão de multas e restrições em caso de descumprimento dos

acordos. Porém, este órgão estaria presente apenas para observar cumprimento de normas vigentes e não como julgador do conteúdo a ser moderado em si (Pallero *et al.*, 2020).

No caso do Google, por exemplo, os serviços foram sendo atualizados desde 2003, com a agregação de várias empresas como Adsense, Android, Urchin e DoubleClick. A plataforma de busca, que domina o mercado de anúncios, tem um algoritmo que estabelece o grau de relevância de um conteúdo para ficar no topo de resultados. No caso das notícias, o SEO organiza o *ranking* não apenas baseado na qualidade da informação, mas principalmente com análise de velocidade de carregamento de site, tamanho das imagens da página, entre outros requisitos técnicos que só podem ser monitorados por um time de profissionais especializados em TI. A maneira como isso vem sendo feito não preza por uma questão primordial: a veracidade das informações e os diferentes pontos de vista, com pluralidade de ideias (Cabrera, 2023).

Em sociedades democráticas há representantes legais que são responsáveis pela elaboração de Leis, com limites constitucionais, que dão legitimidade à regulação. Este arcabouço, segundo Suzor e Gillet (2022), deve prever: adaptação antitruste para a economia de plataforma, mecanismos que abarquem a infraestrutura tecnológica, o tratamento no fluxo de informações privadas e as práticas comerciais. Porém, os autores reforçam que a autorregulação também é um componente necessário na construção dos marcos, com incremento de instrumentos de governança das empresas. Este seria um trabalho contínuo de corregulação, parte exercido pelo estado e a outra pelas plataformas.

Suzor e Gillet (2022) compreendem a autorregulação como uma ação necessária das plataformas, para criar uma cultura própria da sua comunidade de usuários. Alguns problemas precisam ser tratados no âmbito da plataforma, com base em suas normas de oferta do serviço. Usuários precisam ser avisados ao aderir ao serviço que naquele ambiente há limites impostos e uma cultura vigente, caso concorde em participar daquela comunidade. Portanto, atos discricionários, de cumprimento de regras próprias precisariam existir. Neste sentido, o uso da inteligência artificial seria um mecanismo legítimo para aplicação das normas, porém, sem dispensar o elemento humano na ação. Porém, há uma forte pressão internacional e de diversas fontes para que as plataformas sejam mais firmes na repressão de conteúdo prejudicial.

Em termos de políticas públicas em discussão, há uma infinidade de propostas de regulação que passam por: 1) considerar as plataformas como responsáveis intermediárias pelo conteúdo que suportam, sendo obrigadas a retirar material quando citadas, caso do German Network Enforcement Act (NetzDG); 2) cogitar a atuação de públicos reguladores, que obrigariam as plataformas a agirem na retirada de conteúdo, como é o caso da Lei Australiana de Segurança Online; 3) prever a emissão de relatórios periódicos, com vistas à transparência; 4) encorajar a própria indústria da tecnologia a agir, como a “ChristChurch Call”, encampada pela Nova Zelândia no combate ao terrorismo online; 5) focar nas mudanças tecnológicas da internet, que modificam a sociedade muito rapidamente; 6) defender a inclusão da internet na classificação de mídia, como rádio e TV; e, 7) por fim, planejar a criação de comissões de corregulação (Suzor; Gillet, 2022).

Como é possível observar, regulação, autorregulação e corregulação de plataformas digitais são ações em discussão no mundo todo. Um dos pontos cruciais dos debates reside na transparência com que as plataformas coletam e tratam os dados pessoais dos usuários. Este é o tema da próxima seção.

3.3 Transparência na coleta e utilização de dados por parte das plataformas

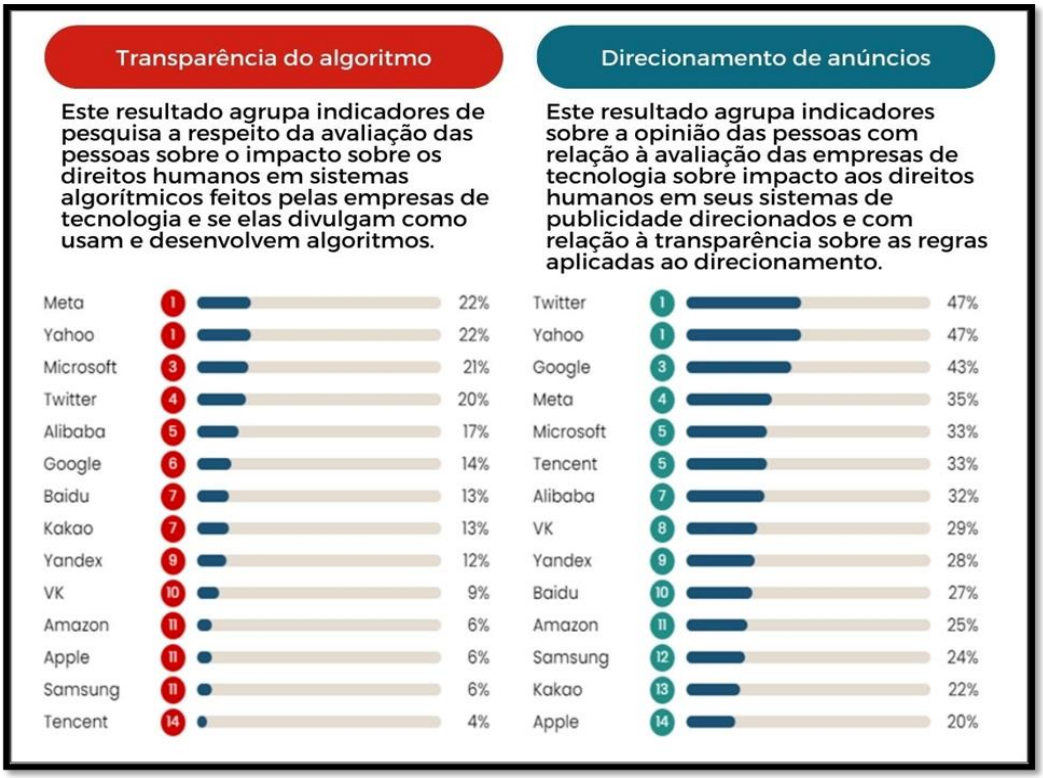
Todo cidadão tem direito à proteção de informações pessoais e liberdade de expressão. O artigo 12º da Declaração Universal dos Direitos Humanos (DUDH) afirma que ninguém pode sofrer invasão arbitrária de sua vida privada, de suas correspondências ou ataques à honra e reputação. A DUDH prevê também a liberdade de opinião e expressão, pensamento, profecia de fé. Reitera, ainda, que ninguém pode ser impedido de emitir sua opinião ou expressar suas ideias, em qualquer meio, independentemente de fronteiras (Assembly, UN, 1948).

A falta de transparência da prática de atividade das plataformas digitais pode levar a conflitos, dificultar a verificação dos fatos e facilitar casos de corrupção e conspiração. Esta realidade é estabelecida porque as plataformas têm oferecido serviços tecnológicos que permitem interações pessoais e compartilhamento de informações em diversos formatos (imagem, texto, áudio ou vídeo), porém, têm falhado em esclarecer o que exatamente pode ser postado em seu ambiente online e como lidam com os dados que coletam de seus usuários (Gorwa, 2019).

Fundada em 2013, a Ranking Digital Rights (RDR) é uma instituição sem fins lucrativos composta por pesquisadores, comunicadores, jornalistas, advogados e tecnicistas espalhados pelo mundo que fazem estudos relacionados à internet e direitos humanos. Os cientistas analisam o processo de confecção dos algoritmos, como é feita a distribuição de anúncios e qual a política de proteção de dados dos usuários. Segundo a RDR (2022), a transparência é a base da prestação de contas tanto de plataformas particulares como de governos, que utilizam os dados dos indivíduos em inúmeros serviços digitais.

O trabalho dos pesquisadores reside no estudo dos efeitos das práticas das plataformas sobre os direitos humanos. Os relatórios anuais, publicados desde 2015, compreendem 300 aspectos sobre transparência, que englobam 58 indicadores baseados na Declaração Universal dos Direitos Humanos da ONU. Os resultados referentes à transparência na aplicação de direitos humanos relacionados à composição de algoritmos e direcionamento de anúncios estão dispostos em um *ranking* das empresas analisadas. Percebe-se que as empresas resistem a revelar a forma como confeccionam seus algoritmos para moderação de conteúdo e direcionamento de propaganda e isso pode ser verificado na Figura 1.

Figura 1 – Avaliação de transparência das plataformas digitais feita pela RDR



Fonte: RDR, 2022, traduzido pela autora. Disponível em: https://rankingdigitalrights.org/index2022/explore Acessado em 24/05/2022.

De acordo com os pesquisadores da RDR (2022), na Meta, dona do Facebook, que é líder de transparência, com 22% dos parâmetros atingidos, os principais problemas encontrados foram: falha em demonstrar a execução de avaliações sistemáticas sobre direitos humanos em aplicações de serviços, práticas publicitárias e sistema algorítmico; apenas os serviços do Facebook e Instagram têm termos de uso, mas com política de publicidade nebulosa; somente dados fragmentados de restrição de conteúdo foram fornecidos e nenhuma informação sobre direcionamento de anúncios; a política de mineração de dados é incompleta, com restrição de possiblidade do usuário ter controle sobre suas informações; a empresa falhou ainda em demonstrar como adquire e processa os dados dos usuários por meio de compra, venda ou acordo de compartilhamento com terceiros.

O Twitter, analisado nesta tese, ficou no topo da transparência da pesquisa feita pela RDR (2022) com relação ao direcionamento de anúncios, porém, obteve 47% de aferição de cumprimento de normas de transparência. No caso do Twitter, os principais problemas encontrados no levantamento da pesquisa foram: insuficiência no fornecimento de informações referentes à diligência com relação aos direitos humanos em suas práticas comerciais; falha em demonstrar avaliações de risco no desenvolvimento de algoritmos; não forneceu informações sobre o processo de abordagem de usuários para remoção de conteúdo e nem sobre violações de dados.

Van Dijck, Poell e De Waal (2018) reforçam que o destino de todo o material coletado é transformado em combustível que alimenta o crescimento das plataformas. A matéria-prima produzida nesta infraestrutura são os dados, que têm sua manipulação e destino opaco. O produto é compartilhado pelas plataformas com terceiros, por meio de APIs,[14] dando aos parceiros métricas e *insights* sobre o comportamento da audiência. Este conhecimento vai ajudar os clientes em estratégias de venda, no desenvolvimento de produtos ou até mesmo na estruturação de novas plataformas.

A promessa das plataformas aos seus clientes é que estes atinjam os anseios e desejos de seu público-alvo. A Airbnb, por exemplo, coleta e processa dados relacionados à hospedagem, mas também funciona como *matchmaker* entre donos de imóveis e interessados em locação temporária. O Twitter oferece serviços de rede

[14] API – abreviatura em inglês para Application Programming Interface, que é um conjunto de comandos e protocolos feito por programadores para a criação de aplicativos e softwares.

social digital, comercializa ainda anúncios e serve de plataforma de venda de produtos (Couldry; Mejias, 2019). A exploração dos dados torna a vida do cidadão transparente, porém, ele é a parte da equação que compartilha informações, não existe uma via de mão dupla.

No ciberespaço uma prática vem se tornando comum, o acesso compartilhado entre plataformas. Caso do Trello, que oferece serviço de organização de trabalho, que autentica entrada de usuários via conta do Google ou Facebook. O usuário não tem ideia do tipo de acordo que há entre as plataformas, faz o acesso para facilitar a navegação, sem ter de preencher um cadastro e senha para o novo serviço. Ananny e Crawford (2018) argumentam que a transparência obrigaria as plataformas a entrar em linha com exigências éticas e legais, trazendo à luz o que os algoritmos escondem. Quanto mais atos fossem distinguidos, maior seria a possibilidade de responsabilização das plataformas pelo tratamento dos dados, porém, há limitações que impedem que apenas a transparência de dados seja suficiente para este efeito positivo.

Nos Estados Unidos, os ideais de transparência foram referência para a criação de normas de administração, legislação – US Administrative Procedures Act, 1946 – e direito à informação – Freedom of Information Act, 1960 –, muito antes das plataformas digitais ocuparem posição de destaque na vida cotidiana dos cidadãos. Estas normas obrigaram o governo a abrir informações sobre mortalidade na saúde pública, índices econômicos, de segurança e compras do governo. Empresas de todos os setores tiveram de se adaptar à abertura de informações nutricionais em embalagens de produtos e utilização de material para pesquisa. Até mesmo entidades de classes profissionais como médicos, advogados e jornalistas criaram suas próprias normas regulatórias para se adaptarem à necessidade de transparência em seus ofícios (Ananny; Crawford, 2018).

Acadêmicos à época classificaram tais ideias de transparência organizacional em três funções: como um valor público de combate à corrupção; como uma referência para tomada de decisões de governos e entidades não-governamentais e, ainda, como uma ferramenta de boa governança. Porém, alguns problemas foram identificados já neste primeiro momento da transparência como:

- falta de credibilidade das fontes;
- responsabilização de danos aplicáveis pela própria entidade que os causou;

- ausência de uma terceira parte que pudesse observar os dados de fora, sem comprometimento hierárquico, de apontamento de erros;
- oferta de informações por evento e não como um processo contínuo de produção de resultados;
- imprecisão quanto ao período de investigação, com informações reveladas *a posteriori* e não em tempo real.

São quatro as formas de transparência nas plataformas: a primeira por iniciativa própria em questões ligadas à liberdade de expressão, que envolve a moderação de conteúdo; a segunda, por decisão judicial, em questionamentos referentes tanto a conteúdo informacional como publicitário; a terceira por normas ligadas a anúncios e a quarta por investigações de terceiros utilizando ferramentas externas (GORWA; ASH, 2020).

Com o passar dos anos, pesquisadores viram as possibilidades de estudos minguarem no ambiente das plataformas digitais. Até 2015 era possível extrair redes sociais completas de usuários do Facebook utilizando aplicativos como Vizster[15]. Passado este período, a plataforma começou a controlar o uso de APIs e muitos perderam funcionalidades ou até mesmo foram extintos, caso do Netvizz[16]. As plataformas se justificaram, por meio de seus engenheiros, afirmando que era difícil criar um algoritmo que fosse transparente e ao mesmo tempo preservasse questões referentes a direitos autorais e privacidade (Hogan, 2016).

Os aplicativos funcionam como *plugs*, que estão conectados às plataformas. Os *apps* extraem os dados e armazenam para consulta ou estratificação e interpretação de informações. Os pesquisadores dependiam das ferramentas externas às plataformas para coletar o corpus de suas pesquisas. A partir do momento que as plataformas desconectaram estes *plugs*, a extração de informação foi encerrada. Novas regras foram impostas, com um estrito controle das plataformas sobre os dados que seriam cedidos, a quantidade, por qual período e para quem se destinavam (Hogan 2016).

A prática de dificultar acesso de APIs externas às plataformas foi intensificada depois dos casos de uso indevido dos dados de usuários para direcionamento de

---

15 Vister. Visualizing online social networks. 2022. Disponível em: http://vis.stanford.edu/jheer/projects/vizster/download.html Acessado em: 05/03/2022.

16 O aplicativo era disponibilizado pelo próprio Facebook até 2018 para extração de redes sociais completas de usuários, porém, foi descontinuado.

informações de campanha eleitoral, nos Estados Unidos e do Brexit, na Inglaterra, pela Cambridge Analytica, fatos descritos no capítulo 2. Estes episódios obrigaram Mark Zuckerberg, CEO do Facebook, a prestar esclarecimentos ao congresso estadunidense. Desde que estes fatos vieram a público, o Facebook tem tentado contornar a crise, oferecendo ao público uma nova Política de Dados implementada pela empresa em abril de 2018 (Semicek; Botelho-Francisco; De Lima, 2021).

> O Facebook, ao estabelecer uma autorregulação para a sua atuação, determina o alcance de sua tecnologia e o controle que estabelece, sem uma interferência governamental que problematize a política de dados. Assim, o escândalo como o de 2018 instiga a empresa a insistir no seu modelo de autorregulação, ao invés de se inserir em um debate sobre regulações externas (p. 135).

Novas possibilidades de pesquisa acadêmica foram abertas, mas com vigilância estrita sobre os dados ofertados. Foram ampliadas normas de autorregulação que definem o que os usuários podem postar e ver na plataforma. Gorwa e Ash (2020), sinalizam que transparência é uma questão política, contestada e frequentemente problemática, porém, ainda assim, importante para remediar situações de injustiça, melhorar a confiança da população em atores centrais na sociedade e valorizar a governança das plataformas. A transparência permite às pessoas compreenderem quando seus direitos individuais foram aviltados e a quem responsabilizar por tal atitude.

Uma das principais justificativas das plataformas para a falta de transparência no compartilhamento de informações sobre os dados coletados é porque entendem que esta matéria-prima lhes pertence, sendo este seu principal produto. O compartilhamento irrestrito é entendido como falha de segurança e até mesmo como risco de exposição de segredo comercial. A maioria das plataformas fornece dados para os quais são inquiridas por autoridades ou terceiros, administrativa ou judicialmente (FINCK, 2018). No que concerne à transparência na coleta e utilização dos dados, engenheiros de sistema atestam que é difícil criar algoritmos que sejam transparentes e ao mesmo tempo preservem questões como propriedade intelectual e privacidade dos indivíduos (Gorwan; Ash, 2020).

As plataformas têm se valido da ausência de regulação para manterem seus lucros, conseguem assim se esquivar do fornecimento de informações, enquanto vigiam e controlam usuários (Balkin, 2017). Cabe aqui um questionamento, quem é de fato dono dos dados, o indivíduo ou a plataforma? A propriedade geralmente é

estabelecida a objetos tangíveis, no caso dos dados, a definição escapa a este critério, porque trata-se de material intangível. Como os termos de uso das plataformas preveem a coleta de dados, subtende-se que as informações seriam delas. As plataformas, porém, foram consideradas controladoras dos dados, mas não proprietárias (Weber, 2017).

O Fórum Econômico Mundial criou uma diferenciação entre os dados. Estas definições podem auxiliar em normas regulatórias que estabeleçam o que as plataformas poderiam coletar:

- **Dados voluntários** - fornecidos de maneira consciente pelo usuário, que sabe quais informações está repassando e quando está transferindo os dados;
- **Dados de observação** - extraídos pelo monitoramento dos hábitos do usuário na plataforma, na maioria dos casos, o indivíduo não está consciente da extração e nem do futuro emprego das informações;
- **Dados de inferência** - obtidos por diferentes fontes, geralmente estão ligados à predição de comportamento ou consumo, o indivíduo não tem consciência da extração e nem controle sobre as informações.

Como os usuários são os verdadeiros donos dos dados, há uma corrente que defende a divisão dos lucros obtidos a partir da utilização das informações. Por esta mesma definição, usuários poderiam fazer a portabilidade de seus dados, como um número de celular trocando de operadora. Naturalmente, a ideia encontra resistência por parte das plataformas que atualmente são as únicas beneficiárias dos lucros gerados pelos dados (Weber, 2017). As plataformas utilizam os dados pessoais dos usuários para impulsionar seus negócios e têm pouca preocupação em como serão explorados por terceiros.

Usuários precisam estar preparados para compreender um pouco melhor como o mercado digital trabalha. Deveriam ler os termos de utilização do serviço para entender quais são os limites das plataformas e fazer valer seus direitos. Uma outra preocupação que concerne os cidadãos reside na utilização de plataformas públicas de ofertas de serviços governamentais online. Novamente, a transparência na prestação do serviço volta à discussão.

3.4 Transparência na coleta e utilização de dados por serviços público e por parte dos governos

O modelo tradicional de regulação dos setores produtivos é feito por comando e controle, com governos estabelecendo regras e empresas cumprindo-as sob pena de multas ou sanções legais. Mas nem sempre os governos respeitam as próprias regras, como o direito à privacidade dos cidadãos. Em 2013, Edward Snowden revelou ao mundo o que o National State of Security (NSA) dos Estados Unidos e o Government Communication Headquarters (GCHQ) da Inglaterra vinham fazendo com dados dos cidadãos ao redor do globo. De acordo com a denúncia, indivíduos eram monitorados, por meio de informações coletadas indiscriminadamente em plataformas como Facebook, Google e Skype. A justificativa para a vigilância foi a luta contra o terrorismo e a violência após o 11 de setembro de 2001, quando uma série de atentados nos Estados Unidos instalou o medo em escala global (Onyeagbako; Adeyoju, 2021).

Quando o assunto é segurança, há uma infinidade de novas tecnologias utilizadas no combate ao crime e ao terrorismo. Vigilância por câmeras, leitores de placas de veículos, drones, programas de reconhecimento facial, inteligência artificial na detecção de indivíduos suspeitos, estas são algumas das ferramentas utilizadas por forças policiais. O avanço tecnológico no setor tornou a privacidade do cidadão um bem cada vez menos valorizado pelo Estado. Uma das situações, já comentadas no capítulo 2, se refere à vigilância de movimentação e conexão dos cidadãos durante a pandemia de Covid-19. É necessário haver um equilíbrio entre necessidade, direitos individuais e responsabilidades (Almeida; Shimarko; Lomas, 2022).

Entre os questionamentos sobre a utilização das novas tecnologias estão: quem deveria desenvolver os sistemas; com que propósitos; para serem usados em quais situações; que tipo de consentimento seria necessário para uso destes equipamentos; como isso seria apresentado à justiça, como seriam estocadas e com quem seriam compartilhadas as informações; como seria o processo de auditagem de dados levantados por inteligência artificial. Nos EUA não há normas regulatórias sobre a utilização destas tecnologias por parte das forças de segurança. O General Data Protection Regulation (GDPR) da União Europeia tem a privacidade no design da utilização de tais aparatos. Porém, quando se trata da aplicação da Lei algumas previsões como consentimento e autorização para utilização de dados não estão sinalizadas. Está mantida, no entanto, a prestação de contas pelo uso (Almeida; Shimarko; Lomas, 2022).

Apenas dois países da UE dispensam o reconhecimento facial para prender suspeitos de crimes: Espanha e Bélgica. O banco de dados da polícia possui uma gigantesca quantidade de imagens de pessoas, algumas envolvidas em crimes e outras que jamais tiveram seus nomes relacionados em qualquer tipo de transgressão legal. Levando-se em consideração que a taxa de acerto é de 99%, ainda sobra 1% de erro. Isso quer dizer que a cada 10000 pessoas inocentes, 100 poderiam ser reconhecidas como suspeitas. Um teste feito em 2018, em Londres, com 104 identificações de suspeitos teve apenas duas confirmações. Na Argentina, no sistema de metrô, 1227 alertas de suspeitos foram emitidos, com a confirmação de 226. Especialistas em sistemas de informação afirmam que o maior problema é a base algorítmica utilizada para a construção do reconhecimento facial, que é opaca (Kayser-Bril, 2021).

Para sociedades democráticas, a vigilância constante de seus cidadãos representa uma quebra de confiança e é contrária aos direitos humanos, porque torna a todos suspeitos por antecipação (Light; Obar, 2019). Publicado anualmente pelo grupo estadunidense de pesquisa Freedom House (2021), o relatório Freedom on the Net verificou que enquanto democracias maduras estão conseguindo tratar de questões de danos online, oferecendo transparência e prestação de contas aos usuários, outros países têm aproveitado o momento para perseguir dissidentes, vigiar cidadãos e fazer propaganda política.

O relatório pontua que governos democráticos devem prever Leis e instituições que sinalizem para práticas corporativas e estatais com princípios que respeitem os direitos humanos, a transparência, prestação de contas e processos legais. O maior perigo reside no Estado ter a capacidade de censurar conteúdo, vigiar e manipular o cidadão, facilitar a corrupção, subverter o processo democrático e reprimir opositores, juntamente com minorias marginalizadas. O relatório de 2021 analisou o nível de liberdade na utilização da internet em 70 países. O estudo compreende:

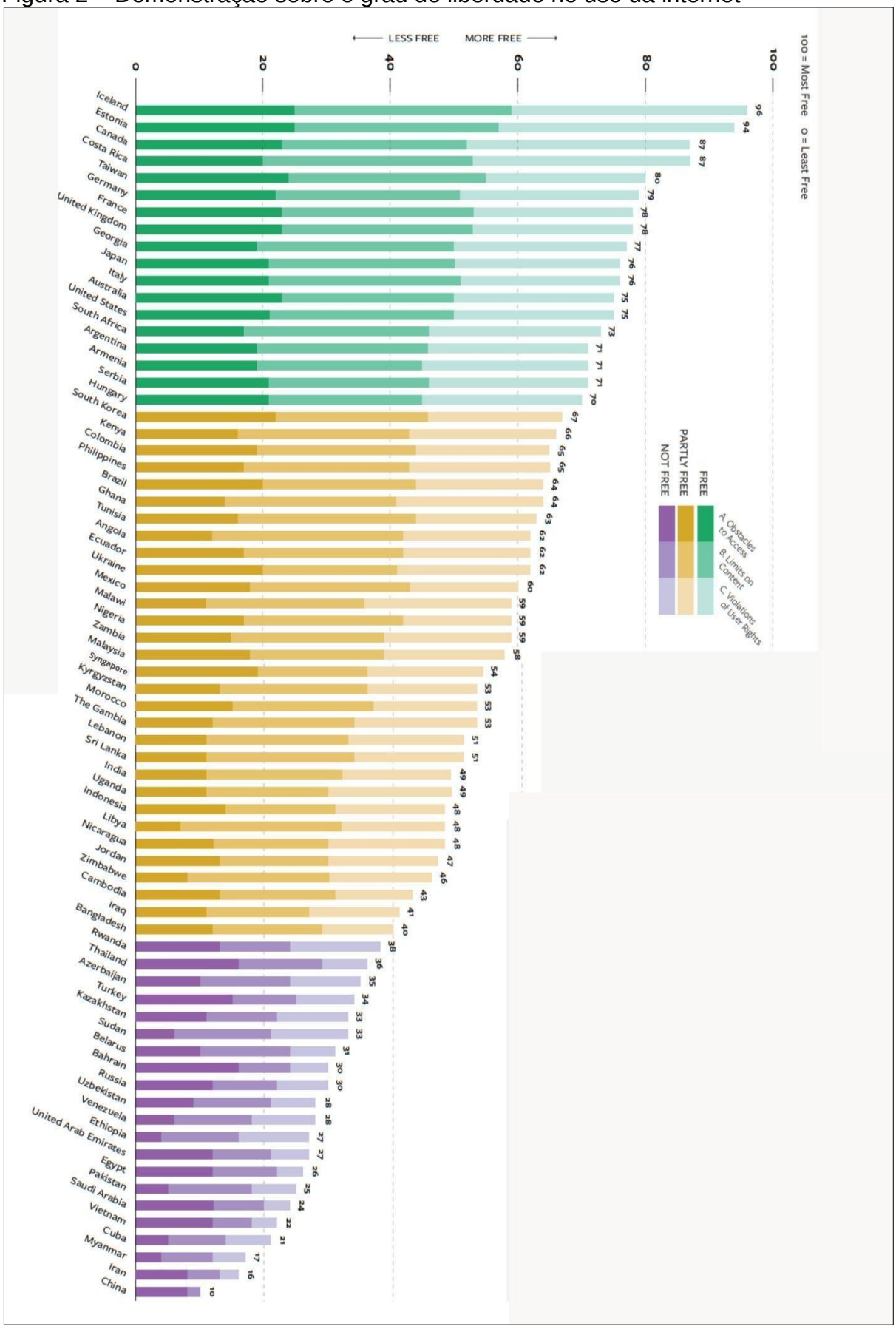
- **Obstáculos de acesso** - barreiras de infraestrutura, econômica e política; decisões governamentais de desligar conexão, bloquear aplicativos ou tecnologias; controle regulatório sobre a propriedade de provedores de serviços de internet; e independência de órgão reguladores.
- **Limites sobre conteúdo** – regulamento sobre conteúdo; filtragem técnica e bloqueio de sites; outras formas de censura e autocensura; diversidade no

ambiente digital; e uso de ferramentas digitais na organização de movimentos sociais.

- **Violações dos direitos dos usuários** – proteção e barreiras para livre manifestação; vigilância governamental; privacidade do cidadão; consequências legais e extralegais para atividades online; ataques físicos ou cibernéticos.

O resultado sobre o grau de liberdade no uso da internet, com o *ranking* dos países analisados segundo os critérios acima citados, está demonstrado na Figura 2.

Figura 2 – Demonstração sobre o grau de liberdade no uso da internet



Fonte: Relatório Freedom on the Net (2021). Disponível em: https://freedomhouse.org

Estados Unidos ficou com a 13ª colocação no *ranking* de liberdade no uso da internet e o Brasil ocupou a 23ª posição. Nos EUA, o resultado relacionado à liberdade caiu pelo quinto ano consecutivo. O avanço da propagação de desinformação na internet culminou com o descrédito do processo eleitoral de 2020 e a invasão do Capitólio, em janeiro de 2021. O Brasil recebeu uma nota positiva por conta do Marco Civil da Internet (Lei 12.965, 2014), que passou por alterações em 2021, e foi considerada uma das Leis mais abrangentes do mundo na proteção aos direitos humanos no ambiente digital. A maior parte dos países da União Europeia ficou bem-posicionada no *ranking*, com Estônia ocupando a segunda colocação. A Islândia, que não faz parte do bloco econômico, ficou pela terceira vez com a primeira colocação, reconhecida pelo melhor ecossistema digital de liberdade e respeito aos direitos humanos (House Freedom, 2021).

A forma como os governos têm lidado com o acesso do cidadão às plataformas digitais tem grande relevância, quando observado o fato de que grande parte dos serviços públicos vêm migrando para a internet. O *E-government* ou Governo 3.0 é uma realidade cada vez mais presente, depois de quase 30 anos do advento da rede mundial de computadores. A transparência na oferta destes serviços é fundamental porque primeiramente o cidadão é vulnerável, frente ao poder do Estado; em segundo lugar, o uso das Tecnologias de Informação e Comunicação (TICs) tem efeito transformativo, com acessibilidade facilitada para a maior parte da população; por fim, é preciso compreender que os objetivos estatais devem ser diferentes das plataformas particulares, que estão sempre em busca de lucro (Ronzhyn; Wimmer, 2019).

De acordo com Ronzhyn e Wimmer (2019), muitos processos governamentais podem ser impossíveis de compreensão pelo cidadão. O relacionamento desigual fica evidente e certas decisões são baseadas exclusivamente em informações colhidas na rede sem ciência e consentimento do cidadão. A prestação de conta no uso de dados colhidos a partir da utilização de serviços públicos precisa existir para que seja mantida a confiança no sistema e processos governamentais. O compartilhamento de informações com terceiros é outra questão que deve ser tratada, com mecanismos que exijam a autorização do indivíduo para utilização. Apesar da internet estar disponível a cerca de 70% da população mundial, a migração dos serviços públicos para o ciberespaço pode representar um risco à acessibilidade de quem não dispõe de meios ou conhecimento para lidar com a tecnologia.

Na China, o Baidu, equivalente do Google, convidou as forças militares para participarem do Brain Project, que desenvolve algoritmos de aprendizagem profunda, utilizando todas as informações dos usuários de navegação na rede e contatos em mídias sociais. A ideia é que cada cidadão chinês tenha seu Citizen Score, um número de identificação no sistema que vai determinar as condições para obtenção de empréstimos, empregos e até viagens internacionais que o indivíduo estará autorizado a fazer. O risco domínio das populações exemplificado por nações totalitárias demonstra que quem controla os algoritmos, pode influenciá-los para se manter no poder. Tecnologias manipuladoras reduzem o poder de escolha do cidadão. A manutenção de regimes democráticos depende de um balanço saudável entre negócios, Estado e cidadãos. Pluralismo e diversidade fazem parte de um ecossistema saudável para federações, com decisões majoritárias (Helbing *et al.*, 2019).

Valle-Cruz (2019) observa que administrativamente, ao fazer a migração de serviços públicos para o ciberespaço, governos estão interessados em demonstrar valores como transparência, eficiência, prestação de contas e inovação. Porém, para gerar no cidadão valores positivos com relação a estes serviços online é preciso garantir a interação, confiança e privacidade. Os maiores entraves no engajamento da população com os *e-services* residem na falta de informações sobre quais são as facilidades que podem ser encontradas em portais ou sites governamentais. Há ainda uma desconfiança com relação à privacidade no compartilhamento dos dados pessoais com o ente governamental na utilização destes serviços e inexistência de interação do governo com os cidadãos.

No Brasil, o decreto 10.332, de 2020 instituiu a Estratégia de Governo Digital de 2020 a 2022. Desde 2016, o País dispunha de mecanismo que normatizava a oferta de transparência do governo no ciberespaço. O decreto que entrou em vigor em 2020 listou 18 objetivos para padronizar a oferta pública dos serviços digitais do País. Entre os objetivos citados no decreto está a solução de problemas relacionados à privacidade dos dados do cidadão. O decreto lista a implementação de segurança da informação e privacidade em ao menos 30 sistemas críticos do Governo Federal até 2022 e ainda a definição de normas padrão de cibersegurança até a mesma data, ou seja, o próprio ente estatal atesta o risco de exposição dos dados dos cidadãos (Brasil, 2020).

Em 2017, 75 países assinaram o acordo Open Government Partnership, para abrir aos seus cidadãos dados administrativos. Porém, o que se percebeu, com o passar dos anos, foi a falta de uniformidade em técnicas de divulgação dos dados e qualidade das informações. A maior parte dos governos têm dificuldade em permitir a participação popular na construção dos dados públicos que serão divulgados. Além disso, são poucas as pessoas que têm condições de analisar os dados públicos, por falta de uma uniformidade na oferta da informação, preparação técnica para o escrutínio dos dados e isso gera uma barreira interpretativa. Os governos, nesse sentido, usufruem de uma transparência nominal, porém não efetiva das informações (Ruijer *et al.*, 2020).

O próximo ponto detalha iniciativas populares de fiscalização e estabelecimento de parâmetros de regulação para a manutenção de direitos individuais.

3.5 Iniciativas provenientes da sociedade para fiscalização da atuação dos governos e das plataformas de mídias sociais sobre liberdades individuais

Criada em 2008, a Global Network Initiative (GNI), agrupou empresas do setor de tecnologia, organizações não governamentais e acadêmicos na tentativa de estabelecer normas para evitar a censura nas plataformas. Em 2010, a Google implementou uma medida para divulgar um relatório com pedidos governamentais para retirada de conteúdo, que permite o acesso público aos dados requisitados. O Twitter passou a publicar seu relatório em 2012, expondo pedidos de informações sobre perfis, para retirada de conteúdo, notificações a respeito de direitos autorais e ainda de remoção por infrações de termos de uso da plataforma. No ano seguinte foi a vez do Facebook dar início a uma publicação bimestral sobre solicitação de dados de usuários por país e remoção de conteúdo enquadrado em descumprimento a Leis locais (Gorwa; Ash, 2020).

Logo depois da denúncia de Snowden, teve início a confecção de um documento, o Internacional Principles on the Application of Human Rights to Communication Surveillance (IPAHRCS). A iniciativa foi referendada por 400 entidades não governamentais e algumas casas legislativas, em países pelo mundo. O documento traz considerações sobre o acesso de governos, juízes e grupos de trabalho internacionais a dados pessoais dos cidadãos. Os princípios estabelecidos serviram de base para a publicação, em 2014, do relatório Right to Privacy in the

Digital Age pela ONU, demonstrando que as normas precisam ser estabelecidas em Leis e ações governamentais no sentido de salvaguardar direitos individuais (Stepanovich; Mitnic, 2015). Veja no Quadro 4 os princípios para a vigilância do Estado a dados pessoais.

Quadro 4 – Princípios para exercício da vigilância estatal

Mecanismos legais	Governos	Justiça
Requisição para vigilância	Deve estar de acordo com Lei vigente, que foi discutida publicamente	A corte que vai analisar a requisição precisa ser imparcial, independente e competente
Necessidade de vigilância	Depois de esgotados meios menos invasivos	Analisar base legal e procedimento formal no pedido, incluindo ônus da prova
Formalização de pedido	Por escrito à justiça, descrevendo a pessoa requisitante e sua função pública	A autorização para vigilância deve prever apenas o escopo necessário para atingir a informação buscada
Conteúdo do pedido ou ordem de vigilância	Deve constar um escopo do que está sendo investigado e quais suspeitas recaem sobre o indivíduo objeto da busca	Deve ser feita por escrito com nomes do concessor e do requerente, Lei que suporta o pedido, metodologia de coleta, escopo da investigação e duração
Ônus da prova	Precisa estabelecer qual ferramenta legal é base da investigação, quais suspeitas existem e em qual suporte espera-se encontrar as evidências	A corte deve acompanhar a investigação e se certificar de que a vigilância está sendo feita dentro do escopo requisitado ao final o material deve ser posto em quarentena e destruído na sequência
Procedimentos de emergência	Devem estar previstos no mecanismo legal as emergências e a requisição precisam preceder a vigilância. Quando a emergência passar, a vigilância deve ser imediatamente suspensa	Analisar a necessidade de aplicação dos procedimentos de emergência, checar a efetividade do mecanismo ao longo do tempo e garantir que o prazo não estenda além do período

Fonte: Elaborado pela autora com base em Stepanovich e Mitnic (2015).

Com relação à coleta de dados para investigação, o IPAHRCS estabelece que: deve respeitar a autorização judicial e não comprometer o funcionamento de servidores; os custos devem ser arcados pelos governos; o pedido às controladoras da informação deve ser feito por escrito, com o nome do requerente, base legal para a busca, metodologia e duração da coleta. Os usuários devem ser notificados da vigilância, salvo em situações justificadas, com risco de perda de provas. Já com

relação aos provedores, eles podem contestar pedidos que estejam em desacordo com a Lei local, ou normas internacionais; devem evitar a criação de sistemas de monitoramento de usuário e precisam manter uma boa higiene de informação (Stepanovich; Mitnic, 2015).

A iniciativa regulatória para prevenir a invasão governamental à privacidade dos cidadãos é mais um motivo para pensar num escopo legal, que previna as plataformas digitais de funcionarem como vigilantes das informações pessoais e censores da liberdade de expressão do indivíduo. Assim como os governos devem ser desencorajados a invadir a privacidade dos cidadãos, empresas particulares também não deveriam se valer de seus serviços para este fim. Quando a World Wide Web completou 28 anos, seu criador, Tim Berners-Lee (2017) afirmou que para cumprir a função para a qual ele a criou, de servir à humanidade, a Internet precisava corrigir três erros que vêm sendo cometidos pelas plataformas digitais. Segundo Lee, era preciso:

1. **Retomar o controle sobre os dados pessoais dos cidadãos**: no atual modelo de negócio, usuários das plataformas não decidem o que querem compartilhar, já que os termos de uso por serviços, ditos gratuitos, não permitem que eles limitem quais informações serão fornecidas. Além disso, o usuário não é consultado sobre o compartilhamento de suas métricas com terceiros e nem conseguem retomar informações já coletadas e processadas. O direito à privacidade acabou e os governos totalitários têm em suas mãos informações que podem levar jornalistas para a cadeia por divulgarem notícias contrárias a seus regimes. Neste sentido, a internet perdeu seu caráter de ambiente de liberdade de expressão;
2. **Criar meios de evitar a disseminação de desinformação:** a forma de distribuição de conteúdo vigente institui a utilização de algoritmos para viralizar *posts*, que são ofertados aos usuários de acordo com seus comportamentos de consumo. Desta forma, a desinformação, na maior parte das vezes, se vale das métricas e é desenhada para a distribuição em massa;
3. **Desenvolver regras claras e transparentes para propaganda política na web:** na atual conjuntura, os anúncios políticos foram transformados em uma verdadeira indústria online. Em 2016, nos EUA, 50.000 anúncios diferentes de um mesmo candidato eram servidos por dia no Facebook, baseados em algoritmos de leitura de comportamento social. Desta forma, a mesma

campanha poderia transmitir mensagens completamente diferentes, apenas para atingir a audiência direcionada.

Para Berners-Lee (2017), a solução do problema não é simples, mas precisa ser discutida. Passa pela negociação das plataformas com seus usuários a respeito dos dados que têm sido coletados e compartilhados com terceiros. Reside também na luta contra governos e plataformas avançando sobre as liberdades individuais, para ter acesso aos dados privados dos cidadãos. E, por fim, um trabalho conjunto entre sociedade e plataformas para combater a disseminação de desinformação sem a criação de uma instituição central com o poder supremo de dizer o que é ou não verdade, na busca pela preservação da liberdade de expressão.

Pouco antes da publicação das críticas de Berners-Lee à World Wide Web, o Instituto de Engenheiros Eletrônicos e Eletricistas dos Estados Unidos colocou em ação, em 2016 o IEEE Global Initiative for Ethical Considerations in AI and AS, em português, Iniciativa Global em Considerações Éticas sobre IA e Sistemas Artificiais (AS). A proposta estabelece que ao criar sistemas de IA ou AS, os desenvolvedores levem em consideração padrões éticos da sociedade que visem melhorar o bem-estar do indivíduo. A proposta foi lançada para que este princípio seja base não apenas de acadêmicos e pesquisadores, mas também, esteja empregado dentro das empresas de tecnologia, como regra de mercado (Chatila *et al.*, 2017).

A primeira versão do documento “Projeto Alinhado Eticamente” foi publicada em dezembro de 2016. Chatila *et al.* (2017) destacam que a peça foi construída a partir da contribuição de 100 pensadores globais nas áreas de IA, robótica, direito e ética, filosofia, academia, governos e do setor corporativo. A ideia principal do documento é servir de base aos desenvolvedores de projeto em IA e AS para a elaboração de projetos, como algoritmos, por exemplo. A iniciativa foi tomada para atender ao mercado, que até a data da publicação não dispunha de um guia prático para desenvolvimento de produtos tecnológicos voltados ao bem-estar da humanidade, priorizando o indivíduo e o convívio comunitário em sociedade. O documento pode ser acessado gratuitamente na web[17].

Para garantir a participação pública na construção de um ambiente ético e saudável é necessário que a sociedade seja parte da composição de uma estrutura

[17] IEEE SA Standards Association. 2022. Disponível em: https://standards.ieee.org/develop/ Acessado em 10/03/2022.

de normas de conduta no ciberespaço. Segundo Janowski e Estevez (2018), as iniciativas populares de regulação dependem de três aspectos principais: implementação de mecanismos estatais que tragam legitimidade às ações, governança a partir de redes de indivíduos envolvidos com as propostas e comprometimento de organizações não governamentais. As iniciativas populares ainda precisam ser validadas pelo governo, para que possam ter sucesso efetivo em suas proposições. Estas iniciativas vão depender de recursos financeiros que possibilitem o investimento em pesquisa, *experts* em tecnologia, espaço para reuniões, formando uma infraestrutura de trabalho voltada a encontrar os termos para a regulação.

Gorwa (2019) partilha da preocupação a respeito da legitimação de iniciativas populares de regulação e sinaliza que este é um caminho necessário na multiplicação de atores capazes de contribuir para a discussão sobre o tema. O autor ressalta que há uma diferença na implementação das iniciativas, quando abrem a possibilidade de aplicação de forma voluntária, daquelas que são impostas por força de Lei. No caso da aplicação de governança voluntária, com normas populares propostas, a negociação é sempre um desafio aos propositores. Pesquisadores como Finck (2018) compartilham da ideia de que a melhor forma de estabelecer parâmetros para regulação seria o desenvolvimento de um escopo de corregulação, no qual as empresas participam, mas precisam respeitar o escrutínio público e governamental.

Algumas iniciativas, seguindo esta lógica, já foram colocadas em ação, este é o caso do GDPR, em vigor na UE. O GDPR foi aprovado em 5 de maio de 2016 e os países membros do bloco europeu tiveram até 6 de maio de 2018 para colocá-lo em prática. O documento foi construído com o passar do tempo, mas enfrentou resistência em seu princípio, quando foi mencionado pela primeira vez, em 2003. A proposta foi rejeitada pela avaliação de que a norma em vigor, datada de 1995, ainda era aplicável aos conflitos da época. A decisão de dar andamento à atualização do arcabouço legal só foi tomada em 2010, quando a Comissão de Mercado Interno Europeu compreendeu que as regras não mais se aplicavam à realidade vigente (Kuner; Bygrave; Docksey, 2020).

O documento foi construído ao longo de quase sete anos com consultas públicas e privadas, grupos de trabalho com cidadãos, empresários, especialistas em proteção de dados, membros dos governos locais, no intuito de englobar normas que compreendessem o cenário contemporâneo. Os principais pontos desta construção

são: direitos ampliados para os titulares dos dados; imposição de notificação de 72 horas após violação de informações; aumento do escopo das responsabilidades das plataformas e ainda imposição de multa de até 4% do lucro global das empresas por descumprimento das normas. As regras são válidas para cidadãos europeus e aplicáveis dentro do território dos 27 países do bloco (Kozlowska, 2018).

Plataformas digitais são obrigadas a oferecer acesso aos dados pessoais aos usuários, com prazo de entrega máximo de 30 dias; devem fazer a atualização de dados, como cadastros, por exemplo; os usuários têm direito ao esquecimento, que deve ser analisado caso a caso, em virtude da natureza da informação e local de armazenamento; o usuário pode restringir o processamento de suas informações; pode fazer a portabilidade de seus registros; e, de acordo com situações particulares, impedir que seus dados sejam processados. A utilização dos dados prevê critérios de responsabilidade, segurança e legalidade. A coleta deve ser feita apenas com um fim específico e as informações guardadas por tempo determinado (De Terwangne, 2020).

A participação popular na construção de normas regulatórias para serem aplicadas às plataformas digitais reforçam a necessidade no avanço da criação de um ciberespaço democrático. Os governos e as plataformas digitais precisam caminhar nesta mesma direção para que sejam mantidos parâmetros de liberdade e privacidade do cidadão na rede. Na próxima seção será tratada a questão dos instrumentos legais de regulação.

3.6 Parâmetros normativos legais e de autorregulação das plataformas para identificação e exclusão de conteúdos de desinformação, conteúdo ilegal e discursos de ódio

No princípio das plataformas digitais, nos Estados Unidos, os administradores se basearam na primeira emenda da Constituição, para afirmar que eram apenas intermediárias e não podiam ser responsabilizadas pelo conteúdo de terceiros postado. Com o passar dos anos, a desculpa vem perdendo sentido. Como já observado, na tentativa de se mostrarem mais transparentes, na última década, as empresas apresentaram normas autorregulatórias que abarcavam política de utilização de seus serviços. Muito do que se avançou até o momento é resultado da insistência governamental e judicial para que as plataformas abram a caixa-preta dos dados (Semicek; Botelho-Francisco; De Lima, 2021).

Balkin (2017) argumenta que o princípio da primeira emenda da Constituição, para proteger as plataformas de responsabilização por conteúdo de terceiros, já não se aplica na sociedade atual. Com dispositivos que permitem um único indivíduo suplantar as mídias tradicionais e propagar sua mensagem com pares ao redor do globo é preciso repensar o paradigma inicial. Já que na atualidade a responsabilidade pela manutenção de uma cultura democrática tem ficado a cargo das plataformas, engenheiros desenvolvedores de algoritmos, legisladores e agências administrativas.

A nova escola da regulação do discurso público sai de um modelo dialógico, no qual havia o Estado interferindo no que o cidadão podia dizer; para um paradigma plural de controle. Neste modelo multifacetado, os cidadãos podem ser monitorados, controlados e censurados tanto pelo Estado, como por diferentes tipos de infraestruturas tecnológicas que não atendem a Leis locais, já que pertencem a empresas transnacionais. Há uma luta por poder e gestão neste ambiente digital, de um lado estão as plataformas que tentam manter a hegemonia de seu domínio das redes sociais e por outro lado estão Estados-nação, que buscam controlar as empresas privadas. A decisão do que indivíduos poderão postar nas redes sociais estará sujeita a quem vencer esta disputa (Balkin, 2017).

Administradores de plataformas atestam que o conteúdo postado passa por um minucioso processo de moderação, que estrutura a participação pública no ambiente digital, com vistas à cooperação e prevenção de abusos. Infere-se, portanto, que a autorregulação tem sido aplicada como regra para o discurso online. Para Correnti (2022) três fatores precisam ser tratados na questão da moderação de conteúdo: consequência aos abusos propagados em conteúdo de mensagens telemáticas; quais os efeitos que podem causar tais mensagens a usuários expostos a elas; e, prejuízos à saúde e segurança, públicos, causados pelo comportamento gerado a partir de tais mensagens.

Neste processo de análise do conteúdo postado nas plataformas digitais estão incluídos administradores e moderadores, que decidem quais conteúdos e usuários serão mantidos, ou retirados; prevê também a participação da comunidade que faz parte do ecossistema, com a possibilidade de denúncias; nota-se ainda uma larga aplicação de algoritmos. Com relação a esta última forma de moderação, vislumbra-se uma ameaça em questões como: tornar o processo de auditoria ainda mais difícil e obscuro; complicar parâmetros referentes à justiça, com defesa de grupos

desfavorecidos em seus discursos; e a possibilidade de politizar ainda mais o ambiente digital (Grimelmman, 2015).

O uso da inteligência artificial foi uma das alternativas apresentadas por Mark Zuckerberg para resolver problemas referentes à moderação de conteúdo no Facebook, como um trabalho que a mão-de-obra humana seria incapaz de realizar. O que se notou a partir desta afirmação no Congresso estadunidense, em 2018, é que a modulação dos algoritmos aumentou em 39% a retirada de conteúdo do ar em Myanmar, por exemplo, em apenas seis meses. O Youtube admitiu que 98% dos vídeos derrubados por violência são obra dos algoritmos. No Twitter a ferramenta AntiSpam é responsável pelo bloqueio de 93% das contas encerradas por divulgação de terrorismo. As plataformas admitem que os algoritmos têm sido cada vez mais empregados na tarefa de moderação de conteúdo. As análises posteriores, de usuários questionando a retirada de *posts* do ar, geralmente são feitas por pessoas contratadas pelas empresas ou em serviço terceirizado (Gorwa; Binns; Katzenbach, 2020).

Twitter modera conteúdo com base em suas normas comunitárias de postagens. Os acadêmicos, porém, criticaram no princípio a falta de clareza para estabelecimento e interpretação das normas. O Twitter abriu aos usuários a possibilidade de acessar informações sobre conteúdo de anúncio direcionado ao perfil do usuário. Por meio do Centro de Transparência da plataforma também é possível acessar os dados de propaganda eleitoral, com detalhamento de valores investidos, doadores e gatilhos de direcionamento de conteúdo. Porém, ainda é problemático receber resposta pelo questionamento sobre *post* derrubados, pedido de verificação de contas e aferição de conteúdo de robôs (Gillespie, 2018).

Helberger, Pierson e Poell (2018) atestam que a responsabilidade pela moderação de conteúdo deve ser compartilhada entre plataformas, usuários e sociedade civil organizada. A complexidade pela determinação se um conteúdo é de fato danoso não pode ser exercida por um único ator. O que ocorre atualmente é a prática de sinalizar o conteúdo, dito inapropriado, usando a técnica de *“flag”,* identificando o *post*. O que determina, no entanto, se o conteúdo terá visibilidade é seu compartilhamento, é neste ponto que o usuário tem um papel importante como distribuidor da mensagem, engajando o público.

Para tentar dirimir o problema o Twitter criou o Twitter´s Trust and Safety Council. Segundo o Twitter, este é um grupo formado por organizações independentes

que desde 2019 presta consultoria à plataforma em assuntos como segurança, assédio, direitos humanos, prevenção ao suicídio, exploração sexual infantil e desumanização. Apesar de apontarem para um caminho de discussão do problema, pesquisadores atestam que os usuários têm pouca participação e responsabilidade no processo (Helberger; Pierson; Poell, 2018).

O maior problema reside no fato de que as plataformas estão numa posição ambígua diante de conteúdo danoso. Conteúdo com teorias conspiratórias, sem fontes confiáveis, muitas vezes viraliza na rede e isso traz dividendos para plataformas e criadores, porque gera engajamento público, audiência. As plataformas negam a intenção de alienar seus usuários e afirmam investir em ferramentas tecnológicas de *"flagging"*, removendo conteúdo do ar, retirando monetização de criadores de conteúdo. O desafio tem sido encontrar um meio termo entre a proteção do ambiente online e a liberdade de expressão, Helberger, Pierson e Poell (2018) fazem uma proposta tripartite de responsabilização, detalhada no Quadro 5.

Quadro 5 – Proposta de apuração de responsabilidades por conteúdo online

Responsabilidades de usuários	**Reponsabilidade das plataformas**	**Responsabilidade dos governos**
- Produzir material diverso	- Criar uma infraestrutura que promova conteúdo diverso	- Estabelecer o papel das plataformas na divulgação de material diverso
- Editar material postado	- Desenvolver meios para envolver usuários na criação e edição de conteúdo existente	- Proteger menores de conteúdo perigoso
- Promover a curadoria de conteúdo	- Produzir ferramentas de manifestação de opinião	- Prevenir a exposição de usuários a conteúdo violento e de ódio
- Curtir, sinalizar e distribuir conteúdo	- Deixar usuário livre para aplicar ou não filtros de conteúdo	- Responsabilizar plataformas na manutenção de regras claras de postagens
- Direcionar conteúdo para grupos determinados	- Oportunizar a criação de fóruns de discussão	- Dar oportunidade aos usuários de se manifestarem na criação de normas regulatórias

Fonte: Elaborado pela autora com base em Helberger, Pierson e Poell (2018)

Na próxima etapa desta tese está descrito o processo de coleta e análise efetiva de Leis, projetos de Leis e normas autorregulatórias elaboradas pelo Twitter. Primeiramente serão apresentadas as normas autorregulatórias e posteriormente foram apresentados os instrumentos legais propostos por Brasil, Estados Unidos e

União Europeia que tratam das questões referentes à moderação de conteúdo, privacidade e segurança do usuário. O capítulo 4 descreve a metodologia de pesquisa, dando detalhes da abordagem de coleta, tratamento e análise do corpus do estudo.

4 – METODOLOGIA

Após apresentação do embasamento teórico, esta tese trata do quadro de análise, que foi desenvolvido a partir de duas etapas metodológicas:

1. Análise de autorregulação: Identifica-se as especificidades das normas autorregulatórias do Twitter sobre liberdade de expressão, traduzida pela plataforma na moderação de conteúdo, posteriormente analisa-se privacidade e segurança, caracterizando-as em relação às normatividades presentes no quadro teórico pertinente.
2. Análise comparativa da regulação: As normas legais de Brasil, EUA e UE foram comparadas com as normas autorregulatórias em quesitos referentes à moderação de conteúdo, privacidade e segurança do usuário, para caracterizar como as normas atuais buscam atender às exigências democráticas de manutenção do direito à informação e comunicação, liberdade de expressão, juntamente com questões referentes à cibersegurança e privacidade do usuário.

Ambas as etapas são desenvolvidas por análise documental, revisão sistemática da literatura e análise de vídeos com palestras e entrevistas concedidas por legisladores e estudiosos, que estão disponíveis, em material audiovisual, no Youtube. A tese utiliza como marco referencial a Hermenêutica de Profundidade (HP) de Thompson (2011), que trata as formas simbólicas inseridas em seus contextos sociais e históricos. “Formas simbólicas são construções significativas que exigem uma interpretação; elas são ações, falas, textos que, por serem construções significativas, podem ser compreendidas” (p. 357).

A HP está dividida em três fases que compreendem a análise sócio-histórica, análise formal ou discursiva e interpretação/reinterpretação (Thompson, 2011). Nesta tese depreende-se que a compreensão e interpretação do processo de autorregulação depende do processo legislativo de regulação das plataformas digitais. O desenvolvimento do estudo utilizando os três instrumentos de balizamento para coleta e análise de dados, serão mais bem detalhados a seguir nos pontos 4.1, que trata do instrumento documental, no 4.2 que detalha o suporte da revisão bibliográfica e o 4.3 que pormenoriza as falas públicas de estudiosos e legisladores.

4.1 Instrumento de análise documental

O levantamento de dados para a pesquisa depende de uma minuciosa busca que contemple documentos divulgados pelo Twitter, compreendendo as normas de autorregulação que utiliza para moderar conteúdo e o que garante ao cidadão, em termos de privacidade e segurança de dados. Faz parte ainda desta etapa o levantamento das normas legais em discussão e em vigência no Brasil, Estados Unidos e União Europeia, a partir do advento do Twitter, no ano de 2006 até o final de 2022.

Este levantamento, tanto das normas de autorregulação, quanto do arcabouço legal utilizado no tratamento da liberdade de expressão, privacidade e segurança do usuário das plataformas digitais é vital para o estudo e para a caracterização do fenômeno social que é analisado. Thompson (2011) destaca que os fenômenos sociais são formas simbólicas, construídas, que devem ser analisadas com um olhar objetivo, quantitativo, que neste estudo caracteriza-se pelo levantamento dos documentos elaborados pelo Twitter e pelos instrumentos legais construídos a partir das casas legislativas. É necessário compreendê-los interpretativamente, de maneira complementar, a partir da visão científica sobre o fenômeno.

Para o levantamento de normas autorregulatórias, opta-se por utilizar a plataforma do Twitter, com informações públicas sobre normas autorregulatórias que balizam a liberdade de expressão, privacidade e segurança do usuário de seus serviços. Foram coletados 18 documentos referentes à Política de Privacidade, outros 17 relacionados aos Termos de Serviço, e mais 43 sobre as políticas do Twitter que foram encontradas em documentos avulsos na plataforma. Estes documentos trataram da forma como o usuário deve se comportar no ambiente ofertado pelo serviço, como a privacidade dele é impactada e quais são as ameaças de segurança a que está sujeito.

No caso das normas legais, foi feito um cruzamento de informações para identificar e delimitar os documentos que seriam coletados. Foram utilizados como fontes de pesquisa o banco de dados das casas legislativas de Brasil, Estados Unidos e União Europeia para a seleção dos documentos. Foram utilizadas palavras-chaves que remetiam a projetos de Lei referentes às plataformas de mídias sociais digitais. Os termos utilizados na consulta foram: mídias sociais, plataformas digitais, provedores de aplicação de internet e provedores de serviços online. As bases de

busca foram os sites do congresso brasileiro (https://www.congressonacional.leg.br/); congresso estadunidense (congress.gov); e parlamento europeu (https://eur-lex.europa.eu/).

Ressalva-se que no Brasil e nos Estados Unidos foram analisados os projetos de Leis e Leis federais, assim como na União Europeia o estudo concentrou-se em Regulamentos e Directivas válidos para o bloco europeu como um todo e não isoladamente por países pertencentes ao território comum. O período de coleta compreende os anos de 2006 a 2022, sendo o marco inicial a criação do Twitter, que publicou sua primeira norma de autorregulação em 2007. No Brasil foram identificados 32 instrumentos legais, sendo 27 projetos de Lei, quatro Leis e uma emenda à constituição. Nos EUA foram listados 95 projetos de Leis e quatro Leis que entraram em vigor. Já na União Europeia foram analisadas seis Directivas e seis Regulamentos aprovados no período delimitado.

Os documentos coletados passaram por um tratamento e foram analisados utilizando algumas assertivas que guiaram a pesquisa, com as seguintes afirmações:

1. Desde quando os temas de autorregulação e normas regulatórias passaram a ser uma realidade para plataformas digitais e casas legislativas.
2. Mudanças identificadas nas normas de autorregulação referentes à moderação de conteúdo, privacidade e segurança do usuário ao longo do tempo e versões publicadas.
3. Mudanças identificadas nas Leis de regulação referentes à moderação de conteúdo, privacidade e segurança do usuário.
4. Contradição e pontos de contato entre as normas autorregulatórias e aos instrumentos legais de regulação referentes à moderação de conteúdo, privacidade e segurança do usuário.
5. Se houve contradição, quais foram os pontos antagônicos entre as normas autorregulatórias e as normas regulatórias referentes à moderação de conteúdo, privacidade e segurança do usuário.
6. Se foram encontrados pontos de contato, quais foram estas congruências que foram demarcadas nas normas regulatórias e de autorregulação.

4.2 Instrumento de revisão sistemática da literatura

A busca nesta fase é encontrar reflexões em interpretações sobre o avanço nos estudos a respeito das normas autorregulatórias das plataformas digitais, assim como do arcabouço legislativo que trata da regulação sobre moderação de conteúdo, privacidade e segurança do usuário. Thompson (2011) salienta que a análise social busca fazer uma interpretação da forma simbólica. Neste sentido, é importante compreender como esta forma simbólica vem sendo interpretada pelos demais pesquisadores do campo-objeto, tornando possível a reinterpretação dos fatos e sujeitos que constroem o mundo sócio-histórico.

Esta reflexão sobre os registros já elaborados a respeito da temática da regulação de plataformas digitais oferece uma retroalimentação sobre o objeto de estudo desta tese. Os resultados anteriormente apresentados dão perspectivas do que é possível avançar, principalmente porque os mecanismos de autorregulação e o arcabouço legal vêm sendo construídos em contexto histórico próprio. Os sujeitos são parte da história e não apenas observadores e "uma nova experiência é sempre assimilada aos resíduos do que passou" (Thompson, 2011, p. 360).

Como a discussão de ideias vem migrando para o ciberespaço, este concentra a liberdade de expressão da contemporaneidade. Para avançar, as sociedades democráticas devem observar critérios de igualdade de espaço, pluralidade de ideias, respeito ao direito à informação e responsabilização pelas informações compartilhadas, assim como, garantir a segurança e privacidade do usuário quando utiliza um meio digital para se manifestar. Thompson (2011) ressalta que é preciso criar parâmetros que tragam objetivos claros na observação de interpretações sobre o campo-objeto. Para isso, foram utilizadas como balizas as seguintes assertivas:

1. Identificação das correntes de estudo quanto à criação de normas autorregulatórias e de regulação das plataformas digitais.
2. Avaliação dos estudos acadêmicos sobre as normas autorregulatórias propostas até o momento pelas plataformas digitais.
3. Avaliação dos estudos acadêmicos sobre a ação dos legisladores no desafio de criar normas regulatórias para as plataformas digitais.
4. Avaliação dos estudos acadêmicos sobre a adequação de normas autorregulatórias e de regulação das plataformas diante das várias demandas de setores sociais, econômicos e políticos.

4.3 Instrumento audiovisual de interpretação de estudiosos e legisladores

A busca nesta etapa da pesquisa é identificar considerações a respeito do que já foi previamente interpretado pelos sujeitos que observam o campo-objeto. Entrevistas e palestras dadas pelos pesquisadores e legisladores sobre os temas em questão proporcionam uma observação mais detalhada a respeito do contexto social em que estão inseridas as pessoas que elaboram e interpretam a regulação de plataforma, abrindo espaço para a reconstrução de tratamento do objeto de estudo.

Foi utilizada nesta fase a ferramenta de detalhamento de pesquisa do Youtube para selecionar materiais audiovisuais mais atualizados com palestras e entrevistas concedidas pelos atores considerados para a análise. As interpretações das formas simbólicas passam pelas opiniões, crenças e contextos sociais em que os sujeitos estão inseridos (Thompson, 2011).

Thompson (2011) chama esta fase de interpretação da doxa, que precisa estar diretamente ligada à análise das condições sociais e históricas em que as formas simbólicas foram estruturadas. É necessário compreender que há contextos diferentes no Brasil, Estados Unidos e União Europeia com relação ao objeto de estudo. Portanto, é preciso detalhar as fases de desenvolvimento da autorregulação e regulação das plataformas, que são heterogêneas, com conjuntos de trajetórias descompassadas. Por isso, os sujeitos envolvidos na interpretação ou construção das normas exemplificam o enquadramento sócio-histórico do tema.

Os sujeitos selecionados para demarcação do momento sócio-histórico são estudiosos da regulação de plataformas digitais e os legisladores que elaboraram as normas legais. Na etapa de análise das normas autorregulatórias são utilizados apenas pesquisadores, os legisladores entram na interpretação dos projetos de Leis e legislações. O estudo visa indicar quais foram as iniciativas que melhor conseguiram equacionar os desafios de oferecer um ciberespaço plural, igualitário e seguro, próprio das sociedades democráticas.

Estão apresentados no Quadro 6 os nomes dos pesquisadores e legisladores selecionados em material audiovisual, com palestras e entrevistas concedidas a respeito das normas autorregulatórias e instrumentos legislativos, com propostas regulatórias que entraram em vigor ou foram discutidas nas casas de Leis dos países e bloco comum selecionados na pesquisa.

Quadro 6 – Pesquisadores e legisladores selecionados para análise de entrevistas no Youtube

BRASIL		
Pesquisadores, políticos e técnicos		
Entrevistado	**Função**	**Vídeos**
Luca Belli	Doutorado em Direito Público - Université Panthéon-Assas (2014). Profº da Fundação Getúlio Vargas, membro do Comitê científico da Computers, Privacy and Data Protection (CPDP) conference e membro do Comitê consultivo da Alliance for Affordable Internet. Pesquisador associado no Centro de Direito Público Comparado da Universidade Paris 2. Trabalhou como agente na Unidade sobre Governança da Internet do Conselho da Europa	Trabalha com a temática da regulação das plataformas digitais. https://portal.fgv.br/combater-aumento-campanhas-desinformacao-mundo-luca-belli
Bia Barbosa	Jornalista e especialista em Direitos Humanos pela Universidade de São Paulo (USP) e mestra em Políticas Públicas pela Fundação Getúlio Vargas (FGV). Integra a Coalizão Direitos na Rede e é conselheira do CGI.br, em uma das vagas do 3º setor	Regulação da mídia: conversa com Bia Barbosa sobre radiodifusão e internet Jornalistas em Luta (30 de maio de 2022) https://www.youtube.com/watch?v=PWlNetnAuaM
Marco Konopacki	Doutor em Ciência Política, Diretor de Governança e Inovação Digital da Defensoria Pública do Rio de Janeiro. Especialista em Governo Digital.	Marco Civil da Internet (Lei 12.965, 2014) Conexão Futura (31 de maio de 2016) https://www.youtube.com/watch?v=m2Hb6YbGkyo
Demi Getschko	Diretor-presidente Núcleo de Informação e Coordenação do Ponto BR. Doutor em engenharia	Marco Civil da Internet (Lei 12.965, 2014) Conexão Futura (31 de maio de 2016) https://www.youtube.com/watch?v=m2Hb6YbGkyo
Alessandro Vieira (CIDADANIA – CE)	Senador do CIDADANIA pelo Ceará.	PL das Fake News Flow (8 de maio 2023) https://www.youtube.com/watch?v=nowy-UxM7fI&t=822s acessado
ESTADOS UNIDOS		
Pesquisadores, políticos e técnicos		
Entrevistado	**Função**	**Vídeos**
Daphne Keller	Formada pela Yale Law School, Brown University e Head Start, foi Diretora de Responsabilidade	Daphne Keller of the Stanford Cyber Policy on “Who Controls Online

	Intermediária no Centro de Internet e Sociedade de Stanford até 2020	Speech" (April 22, 2020) UCLA School of Law https://www.youtube.com/watch?v=vhyeJ2RelJI Regulação de plataformas: Os modelos de negócios das plataformas NICbrvídeos (20 de maio de 2021) https://www.youtube.com/watch?v=HqVBD2st6SE
Tarleton Gillespie	Pesquisador da Microsoft, profº associado da Universidade de Cornell em Comunicação e Ciência da Informação, com uma nomeação em pós-graduação em Estudo de Ciência e Tecnologia, tem mestrado (1997) e doutorado (2002) pela Universidade da Califórnia	Do not recommend: How platforms reduce the visibility of some content, and why Digital Society (16 de dezembro de 2021) https://www.youtube.com/watch?v=a-CZpIIKaco "Do Not Recommend: Reduction Techniques, as a Form of Moderation"' DIMACS Workshop on Computer Science and Law (20 de maior de 2022) https://www.youtube.com/watch?v=WZbI9L7AfXM
Nada Anajafi	Pesquisadora, autora de livro e advogada, especialista em contratos.	Twitter terms of service (19 de fevereiro de 2021) https://www.youtube.com/watch?v=RMlkr2dckSU
Cathy Gellis	Ex-programadora, advogada especialista em Internet	What is the NUDGE Act? (16 fev. 2022) https://twit.tv/shows/this-week-in-google/episodes/651
Amy Webb	Diretor Executivo da FTI, Autora dos livros The Big Nine [futuros da IA] e The Genesis Machine [futuros da Synbio] • Futurista Quantitativo • Prof, NYU Stern.	New Bill Aims to Change Algorithmic Feeds. (20 fev. 2022) https://twit.tv/shows/this-week-in-google/episodes/651 Acessado em: 07/06/2023.
Paris Martineau	Repórter na The Information	New Bill Aims to Change Algorithmic Feeds. (20 fev. 2022) https://twit.tv/shows/this-week-in-google/episodes/651 Acessado em: 07/06/2023

Jan Edwards	Fundadora e presidente da Paving the Way Foundation que trabalha no campo da educação preventiva e programas de conscientização para interromper o ciclo do tráfico humano	Three Kids' Internet Safety Bills You Need to Know. (16 set. 2022) https://www.youtube.com/watch?v=5bSuNfjqWNc Acessado em: 13/06/2023.
Rick Lane	Rick Lane é o fundador e CEO da Iggy Ventures, LLC, que se concentra em aconselhar e investir em startups, projetos e iniciativas de políticas públicas de impacto social positivo	Three Kids' Internet Safety Bills You Need to Know. (16 set. 2022) https://www.youtube.com/watch?v=5bSuNfjqWNc Acessado em: 13/06/2023.
Marsha Blackburn (PR – MS)	Senadora Republicana pelo Estado da Tennessee	EXCLUSIVE: Sens. Blackburn and Blumenthal Join Forbes to Discuss Bill to Keep Kids Safe Online (16 mar. 2023) https://www.youtube.com/watch?v=y8UsgNcOwho Acessado em: 15/06/2023.
Richard Blumenthal (PD – NY)	Senador Democrata pelo Estado de Connecticut	EXCLUSIVE: Sens. Blackburn and Blumenthal Join Forbes to Discuss Bill to Keep Kids Safe Online (16 mar. 2023) https://www.youtube.com/watch?v=y8UsgNcOwho Acessado em: 15/06/2023.
Emily Birnbaum	Repórter da Bloomberg News trabalha principalmente com cobertura legislativa	What Is the SMART Act? https://www.youtube.com/watch?v=o001s-n-etE Acessado em: 16/06/2023.
Harry MacCracken	Jornalista, editor de Tecnologia da Fast Company, ex-editor da Time e ex-editor da Technologizer	Craigslist Personals Shut Down Due to SESTA/FOSTA 26 mar. 2018 *https://www.youtube.com/watch?v=FO_xBuhh24E Acessado em: 21/06/2023.*
Denise Howell	Advogada de direito digital e colunista do ABA Journal, California Lawyer, Law Technology News, Law.com, The Lawyer's Guide to Marketing on The Internet, e em "The Screen Savers" (TechTV) e "Life and Times"	Craigslist Personals Shut Down Due to SESTA/FOSTA 26 mar. 2018 *https://www.youtube.com/watch?v=FO_xBuhh24E Acessado em: 21/06/2023.*
Iain Thomson	Jornalista editor The Register	Craigslist Personals Shut Down Due to SESTA/FOSTA 26 mar. 2018 *https://www.youtube.com/watch?v=FO_xBuhh24E Acessado em: 21/06/2023.*

Harold Feld	Vice-presidente da Public Knowledge, autor do livro “The Case for the Digital Platform Act”, advogado e colunista	The Case for the Digital Platform Act. PdF YouTube, 28 de jun. 2019. https://www.youtube.com/watch?v=UyRQLmKZQAA&t=82s Acessado: 23/06/2023.
Sam Altman	Presidente da Y Combinator, copresidente da OpenAI, criador do ChatGPT	OpenAI CEO, CTO on risks and how AI will reshape society. ABC News, 17 mar. de 2023. https://www.youtube.com/watch?v=540vzMlf-54 Acessado em: 26/06/2023.
UNIÃO EUROPEIA		
Pesquisadores, políticos e técnicos		
Entrevistado	**Função**	**Vídeos**
José Van Dijck	Autora de livros sobre novas mídias, é professora da Universidade de Utrecht, na Holanda, desde 2017. Por 15 anos foi professora de Estudos da Mídia, na Universidade de Humanidade de Amsterdã. Recebeu em 2019, da Universidade de Lund (Suécia), um doutorado honorário por seus méritos científicos.	1- A European Perspective on Platformization Università di Siena DISPOC (26 de abril de 2022) https://www.youtube.com/watch?v=Jiss8LsKwv0 2- Obsessie met data schadelik voor het goede leven. (Youtube, 25 de jun. de 2021) https://www.youtube.com/watch?v=ZLYhdXU3TNA&t=292s
Robert Gorwa	Pesquisador PHD da WZB Berlin Social Science Center, da Center For Democracy and Technology (CDT) e Centre for International Governance Innovation (CIGI).	PANEL A1: PLATFORM GOVERNANCE Giganet (13 de agosto de 2021) https://www.youtube.com/watch?v=TQTPFNAT9pk
Jonas Valente	Pesquisador do Laboratório de Políticas de Comunicação da UnB e no Oxford Internet Institute.	Especialistas comentam a regulação do audiovisual (26 de julho de 2021) https://www.youtube.com/watch?v=GpnmMGfHApw
Jorge Martins	Advogado especialista em tecnologia	Factos e mitos sobre o RGPD / LGPD (Lei Nº 13.7096, 2018)– Portugal (22 de novembro de 2019) https://www.youtube.com/watch?v=in39ZdE4U64
Roberto Viola	Diretor-Geral para Comunicação, Conteúdo e Tecnologia da Comissão Europeia	#EUpeople: behind the scenes with Roberto Viola (19 de janeiro de 2019)

		https://www.youtube.com/watch?v=P_FlxGpe_NI 2 - Roberto Viola (DG CNECT) on digital transformation and its impact on society (12 de maio de 2022) https://www.youtube.com/watch?v=QWOoqe9tZw4

Fonte: Elaborado pela autora

Nesta etapa, as assertivas balizadoras são:

1. Observação de opiniões dos pesquisadores sobre a regulação das plataformas digitais.
2. Crenças dos pesquisadores sobre o direcionamento que tem tomado a regulação ou a falta de regulação das plataformas, que interfere nas sociedades democráticas.
3. Perspectiva dos pesquisadores sobre o futuro da regulação de plataformas digitais.

ANÁLISE DE DADOS

5 – NORMAS AUTORREGULATÓRIAS E LEGAIS

Desde 1948, a Declaração Universal dos Direitos Humanos prevê que todo ser humano tem direito à liberdade de expressão, comunicação e informação em qualquer meio de difusão de ideias. Em 5 de julho de 2012, o Conselho de Direitos Humanos da ONU aprovou uma resolução, apresentada pela Suécia, para garantir os direitos humanos na internet. A medida, apoiada por 70 países, membros e não membros, instituiu que os direitos offline deveriam ser respeitados também online, em particular a liberdade de expressão, aplicável independentemente de fronteiras. A resolução coaduna com a DUDH e com o Pacto sobre Direitos Civis e Políticos (Benedek; Ketlemann, 2020).

Os maiores desafios desta resolução, porém, são as características da própria internet, que é descentralizada, com um entrave de ação ampliado para a manutenção dos mesmos parâmetros online para responsabilização de usuários extremistas. Nota-se a complexidade, por exemplo, para a penalização de violadores de direitos humanos, abusadores de crianças e terroristas (Benedek; Ketlemann, 2020).

Neste capítulo da tese são analisadas as normas autorregulatórias do Twitter e o arcabouço legal de Brasil, Estados Unidos e União Europeia. A primeira Política de Privacidade do Twitter foi confeccionada em 2007, a partir de Leis já vigentes e cinco projetos de Leis que haviam sido discutidos nas casas de leis estadunidenses no ano anterior à elaboração da norma. Esta tese afirma que as normas autorregulatórias utilizam projetos de Leis em discussão como base temática de suas propostas. É notório que discussões legislativas partem dos anseios da sociedade, porém, esta tese não se propõe a investigar manifestações populares ou fatos que deram causa a projetos de Leis.

Questões como liberdade de expressão no ciberespaço, privacidade e segurança do usuário na rede receberam maior atenção conforme as atividades cotidianas foram sendo transferidas majoritariamente para as plataformas digitais. Legisladores foram compelidos a tratar dos mais variados temas em projetos de Lei que muitas vezes não saíram das tribunas das casas de Leis, mas acabaram servindo de base para a confecção de normas autorregulatórias. Com o passar do tempo, as plataformas digitais também ganharam protagonismo em processos eleitorais, criando

um desafio ainda maior aos legisladores para a manutenção de um ambiente online diverso, minimizando ameaças aos sistemas democráticos.

A seção 5.1 trata do histórico das normas autorregulatórias, como surgiram e como ganharam complexidade nas regras com o passar dos anos. A seção 5.2 está destinada ao resumo dos 16 anos de normas e os 78 documentos apresentados. O arcabouço legal é detalhado na seção 5.3, que trouxe o regramento proposto para as plataformas digitais nas mais diversas temáticas. Na seção 5.4 apresenta-se a síntese de 143 instrumentos legislativos que compreendem uma emenda a CF (1988), brasileira, Leis, projetos de Leis, Directivas e Regulamentos discutidos no Brasil, EUA e UE no período selecionado. Por fim, as normas regulatórias são analisadas em comparação com as autorregulatórias, fazendo assim um cruzamento de informações e demonstrando como o movimento legislativo impulsiona a autorregulação das plataformas na seção 5.5.

5.1 Normas autorregulatórias do Twitter

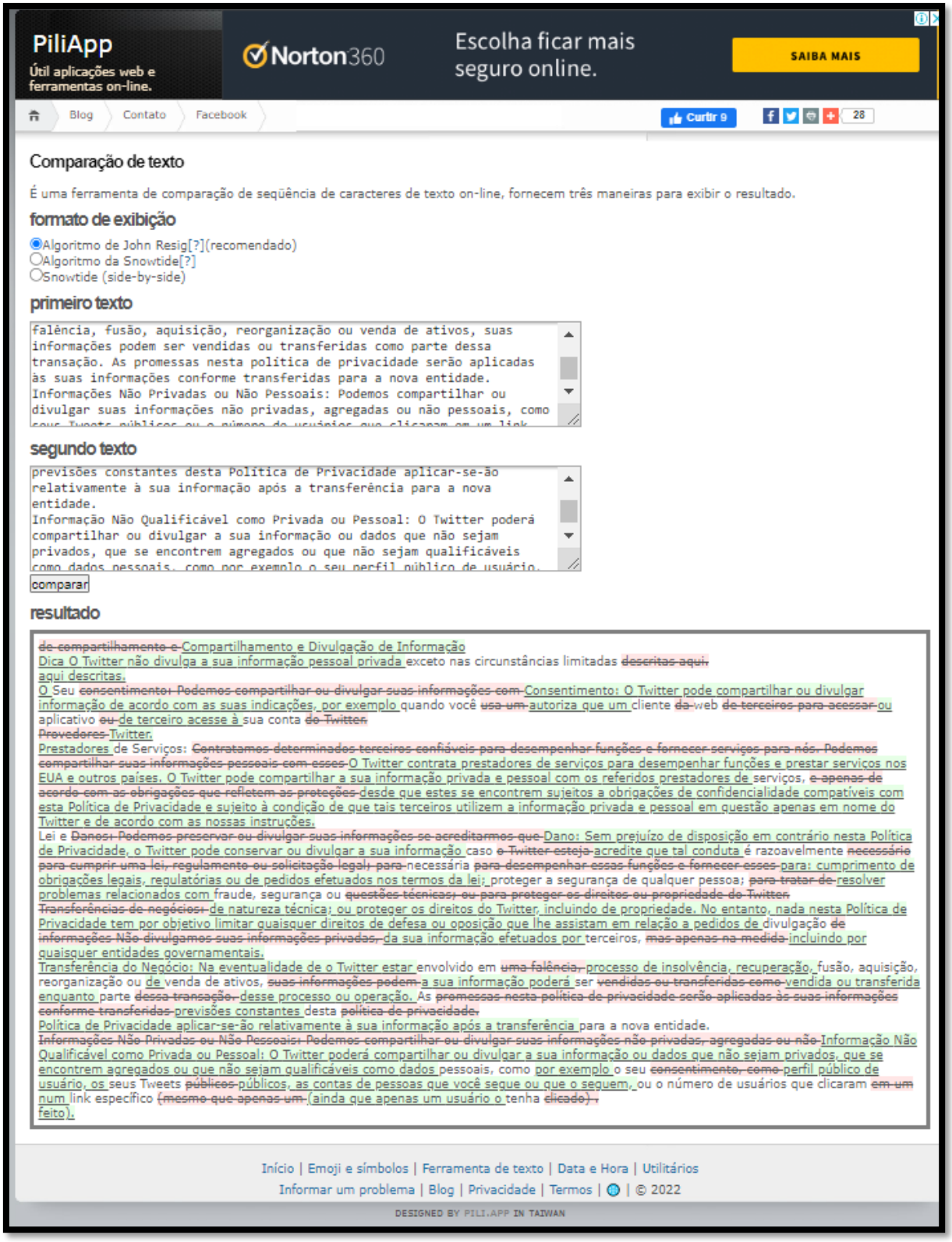
O Twitter deu início à divulgação de suas normas autorregulatórias no ano de 2007, com a publicação da Política de Privacidade (PP), que também incluiu detalhes sobre a segurança do usuário. Uma lacuna de dois anos entre a primeira publicação e a segunda foi registrada. Apenas em 2009 a plataforma passa a publicar os Termos de Serviço (TS). Neste mesmo ano, o TS recebe duas adequações e a PP de número 2 passa a vigorar. Ao todo, até o ano de 2022, a PP apresentou 18 versões, enquanto os TS 17. Os arquivos permanecem disponíveis para consulta no site do Twitter. No cabeçalho introdutório de cada documento consta a informação de que aquela é uma versão já descontinuada pela plataforma e o link para a versão mais atualizada é disponibilizado.

Para análise das mudanças ocorridas nos documentos com o passar do tempo foi utilizado o site PiliApp para comparar os textos. O serviço oferecido pelo site funciona como um identificador de plágio que aponta trechos inalterados e os alterados de cada texto. No caso desta tese optou-se pelo algoritmo John Resign,[18] que aplica a comparação de textos riscando em marrom as informações suprimidas e incluindo em verde as adicionadas, a escrita preservada é mantida na cor original,

[18] De acordo com seu perfil no Twitter, John Resign é um arquiteto de softwares da Khanacademy.

preto. A ação da ferramenta pode ser conferida na captação de tela do computador compartilhada na Figura 3.

Figura 3 – Site PiliApp utilizado para fazer comparação de textos



Fonte: Captura de tela do site PiliApp. Disponível em: https://pt.piliapp.com/text-diff/#diff acessado em 09/07/2022

Até a versão 5 da PP e versão 6 dos TS, os documentos estão disponíveis apenas em inglês, no site do Twitter no Brasil. A partir da versão 6 da PP e 7 dos TS os arquivos são encontrados em português. No caso particular da comparação entre a versão 5 e 6 da PP e 7 e 8 dos TS foi feita a tradução da versão 5 da PP e 6 dos TS. Por conta da necessidade de tradução do texto, o foco ficou centrado nas mudanças semânticas das informações. Políticas de Privacidade estão detalhadas na seção 5.1.1., as mudanças ocorridas nos TS na sequência na seção 5.1.2. Ao final apresenta-se um quadro de resumo das principais mudanças em ambos os documentos ao longo dos anos.

Com o passar do tempo notou-se que a mudança nas PPs e TSs ficou cada vez menor, porém, a plataforma encontrou uma outra maneira de se autorregular. Documentos avulsos foram sendo introduzidos em links externos às Políticas de Privacidade e Termos de Serviço, com respostas às demandas legislativas e estas normas foram espalhadas pela plataforma. Este movimento autorregulatório tornou a vida do usuário cada vez mais complicada. Os documentos avulsos de autorregulação do Twitter referentes à liberdade de expressão, privacidade e segurança foram analisados na seção 5.1.3. e totalizaram mais 43 documentos.

5.1.1 Política de Privacidade (PP)

A primeira PP que foi publicada tinha apenas três páginas, com linguagem simplificada. O documento especificou que o Twitter faria o processamento das informações pessoais de quem subscrevesse a plataforma. Processamento de informação foi definido na peça escrita como ação de coleta, armazenamento, exclusão, utilização, combinação e divulgação dos dados, especificando os Estados Unidos como base para estas atividades. O uso de *cookies*[19] também fazia parte do *modus operandi* da empresa, que justificou sua ação como forma de melhor identificar seus usuários e com isso oferecer um serviço personalizado (Twitter, 2007).

Van Dijck (2021) observa a forma de atuação do Twitter e de outras plataformas com preocupação. Ela utilizou o termo datificação para traduzir a interação social e o movimento físico em dados, como um pedômetro, que identifica as pegadas digitais no ciberespaço. Utilizou ainda dataísmo, que seria a crença de que os dados são

[19] O *cookie* é um arquivo de texto simples armazenado pelo navegador, sua função é guardar as informações de navegação do usuário na web.

transferidos com um fim determinado, que pode inclusive ser medido, transformando-se em uma realidade objetiva de finalidade. Desta forma, a vigilância de comportamento vai se aprofundando à medida que mais informações são coletadas, processadas e armazenadas, num comportamento de vigilância constante, que se sustenta por medir, manipular e monetizar.

É possível identificar este comportamento do Twitter pela quantidade de informações admitidas pela plataforma como matéria prima desde o princípio dos documentos que registram este *modus operandi*. O processamento das informações do usuário incluía: endereço de IP, nome de usuário, senha, endereço de e-mail, cidade, fuso horário, número de telefone e qualquer dado divulgado na *bio* do perfil público montado na plataforma. O Twitter reiterou que poderia utilizar as informações para direcionamento de publicidade e oferta de serviços, inclusive utilizando dados sobre a navegação na internet coletada pelo programa Log Data (Twitter, 2007).

Empresas contratadas para hospedagem, manutenção, relacionamento com o cliente, armazenamento e gerenciamento do banco de dados e campanhas de marketing direto teriam acesso aos dados de usuários. Além disso, informações poderiam ser compartilhadas com governos, autoridades policiais até entidades privadas no cumprimento de Leis e ações de investigação. De acordo com a plataforma, a intenção neste caso seria a prevenção à ocorrência de atividade ilegal, antiética ou que interferisse em segurança (Twitter, 2007).

Em caso de venda do Twitter foi previsto que a empresa adquirente seria a nova detentora dos dados dos usuários, que poderiam se opor à transferência. Por fim, a empresa informou que dispunha de barreiras criptográficas para que as informações dos usuários fossem resguardadas. Porém, não haveria endosso da plataforma a links compartilhados. O uso da plataforma foi indicado para maiores de 13 anos (Twitter, 2007).

Para Van Dijck (2022), o maior entrave à democracia contemporânea reside na utilização dos dados pessoais do cidadão, que têm suas vidas privadas sob o domínio de empresas particulares desde muito cedo. A pesquisadora criou a figura de uma árvore digital para facilitar a visualização da importância das plataformas e o risco do domínio que exercem sobre a vida cotidiana da sociedade. Os provedores de internet estariam nas raízes, dando base à infraestrutura do sistema. As redes sociais estariam no tronco, sendo a parte mais importante que permite a dominação da esfera pública

pelas companhias de tecnologia, porque muitas atividades da vida passam pelas plataformas.

Para garantir que as pessoas fossem mantidas no tronco de sua rede, o Twitter lançou a segunda versão da PP em 2009. O documento adicionou a possibilidade de tratamento de dados advindos de vários sites e serviços ligados à plataforma, em qualquer país que a empresa operasse e como ramos de atuação houve um aumento significativo de dados que seriam coletados. Dúvidas poderiam ser endereçadas ao e-mail privacy@Twitter.com. Foram adicionadas Tips,[20] a primeira trazia a seguinte frase: “Nós coletamos e usamos suas informações para oferecer nosso Serviço e melhorá-lo com o passar do tempo” (Twitter, 2009d).

A versão 2 da PP deixou claro que biografia, local de residência, foto de identificação eram informações públicas, assim como, lista dos perfis seguidos pelo usuário, tweets marcados ou “retweetados”. Além disso, todos os tweets postados poderiam ser distribuídos não só na plataforma, mas também por SMS. A partir destas informações mais uma Tip foi publicada com a seguinte frase: “O que você diz no Twitter pode ser visto imediatamente ao redor do mundo” (Twitter, 2009d).

Os serviços do Google Analytics foram citados como fonte para estratificação da utilização da plataforma. Por consequência, dados do usuário eram compartilhados com o Google para aferição de métricas. Mais uma Tip trouxe a tônica da evolução da PP: “Nós não divulgamos suas informações privadas, exceto nos limites descritos aqui”. Uma série de detalhes foram expostos referente a:

- Consentimento do usuário, quando acessasse a plataforma via terceiros (como Google, por exemplo);
- Compartilhamento de dados com parceiros;
- Divulgação de informação para atender à Lei, regulação ou investigação, na busca de proteger qualquer pessoa, para tratar de fraude, segurança técnica ou direitos de propriedade do Twitter;
- Transferência dos dados do usuário como produto, em caso de venda da plataforma;
- Informações públicas como tweets e cliques do usuário também estavam previstos como material de compartilhamento e divulgação da plataforma.

[20] Tips em tradução livre são dicas.

A terceira versão da PP trouxe apenas duas adições: o monitoramento da atividade do usuário referente ao clique em links em tweets e a informação de que o Twitter mantinha um variado serviço de hospedagem, com parceiros, inclusive o Google. Com isso, o usuário estava exposto ao compartilhamento de seu IP e instalação de *cookies* em sua máquina (Twitter, 2010a). No mesmo ano, o Twitter informou que monitorava a navegação do usuário não só em sua plataforma, mas também nas de parceiros (Twitter, 2010b).

Poucas alterações foram feitas na PP 5, as principais mudanças de monitoramento foram a adição de *widget*[21] em websites pessoais e aplicações como Twitter para Mac, Twitter para Android ou TweetDeck, com coleta de dados da operadora de celular utilizada pelo usuário e IDs de dispositivos e App instalados. A instrução acrescentou que a empresa teria discricionariedade na exclusão dos dados do usuário em 18 meses e na cessão de informações sensíveis para cumprimento de Lei, regulação ou investigação. O Twitter informou que após a exclusão de uma conta, feita a pedido do usuário, o perfil ficaria desativado, podendo ser recuperado em 30 dias (Twitter, 2011b).

A PP 6 alertou o usuário que suas informações seriam utilizadas para encontrá-lo na rede e para oferecer perfis semelhantes para interação. Perfis de outras redes sociais, conectadas à conta do Twitter, também teriam dados compartilhados entre as empresas. Foram incluídas informações sobre o monitoramento de localização do usuário pela utilização do Twitter no celular e permissão para desativação de cookies. O Twitter aderiu ao Safe Harbor Principles of Privacy, acordo feito entre EUA, UE e Suíça, “relativos ao aviso, escolha, transferência, segurança, integridade de dados, acesso e aplicação” (Twitter, 2012a).

O Safe Harbor trata da proteção dos dados dos cidadãos da UE. O artigo 25 do documento impede que qualquer país membro do bloco permita o tratamento de dados de seus cidadãos em países onde não exista uma política de privacidade em vigor. Em novembro de 2013, a Comissão Europeia fez uma revisão no acordo, que estava em vigor desde o ano 2000 e percebeu que vários estados membros não estavam cumprindo com o acordo, o que impôs algumas ações de mediação de conflitos (Connolly; Dijk, 2016).

---

21 Widget é uma interface gráfica utilizada para simplificar o acesso a aplicativos, programas ou sistemas.

A 7ª versão da PP incluiu a customização de anúncios sobre produtos e serviços mediante monitoramento de navegação de empresas parceiras do Twitter. O usuário foi alertado que poderia impedir este monitoramento por meio da ferramenta Do Not Track (Twitter, 2013a). Na PP 8 o Twitter especificou que recebia informações do usuário também de anúncios, parceiros e terceiros (Twitter, 2013b). A PP de número 9 adicionou a possibilidade de cessão de dados para pesquisas acadêmicas, análise de tendências e percepções, inclusive por agências de saúde. Foi admitido o monitoramento de dados de torres de operadoras ou redes sem fio, inclusive em *downloads* de apps. A plataforma reconheceu a coleta de informações de cartão de crédito, com exceção do local de entrega da compra e CVV[22], que ficariam disponíveis aos prestadores do serviço ou vendedores dos produtos para conclusão do negócio e facilitação na verificação de litígios e/ou fraudes (Twitter, 2014a).

De acordo com a PP 10, moradores dos EUA manteriam como administradora de seus dados a Twitter Inc, com base em São Francisco, na Califórnia. Já para os demais usuários, os dados ficariam sob a tutela da Twitter Internacional Company, em Dublin, na Irlanda. A empresa explicitou que o usuário poderia utilizar a conta sob um pseudônimo, prática que já era comum na plataforma. Com base nos tweets postados e "retweetados" pelo usuário, a plataforma admitiu que poderia direcionar conteúdo e perfis semelhantes. Afinal, a plataforma admitiu o compartilhamento dos dados com terceirizados contratados para prestação de serviços (Twitter, 2015a).

Para Benedek e Kettemann (2020) a condição de anonimato nas redes sociais pode ser essencial para críticos de governos totalitários. Um exemplo da necessidade de manutenção do anonimato online são os casos de denúncia de governos corruptos, que com frequência são suportados pela condição de anonimato dos denunciantes. Porém, cada situação necessita de análise individual, porque o anonimato também pode ser utilizado para agredir pessoas como a campanha antissemita, registrada na França em 2013.

Em 24 de janeiro de 2013, um tribunal francês convocou o Twitter para identificar e notificar usuários que estavam divulgando mensagens antissemitas, indexando seus posts sob a *hatshtag* #unbonjuif – algo como #umbomjudeu – que vinham acompanhados de ameaças de morte, extermínio, entre outras ofensas. A

[22] A sigla CVV quer dizer Card Verification Value e refere-se a três números que estão na parte de trás dos cartões de crédito. Estes números são utilizados para as compras via internet e atestam que o dono está em posse do cartão de crédito no momento da compra.

decisão judicial foi proferida depois que o Sindicato dos Estudantes Judeus da França processou a plataforma por não tratar da utilização do seu ciberespaço como ambiente de ataque à comunidade judia e por não lidar com o problema, mesmo depois das denúncias da comunidade (Benedek; Ketlemann, 2020).

Somente a partir da versão 11 o Twitter especificou que cabia ao usuário atentar para o conteúdo que postasse, observando os Termos de Serviço e as Normas do Twitter. A empresa admitiu que a transferência e processamento dos dados poderiam ser feitos tanto nos EUA, quanto na Irlanda, ou em qualquer outra localidade de operação da plataforma. Um adendo trouxe a informação de que as leis de privacidade de dados poderiam ser diferentes entre EUA, Irlanda e o país de residência do usuário. Para dirimir dúvidas, o endereço de e-mail privacy@Twitter.com foi divulgado como canal para esclarecimentos. A adesão às regras do Safe Harbor Principles of Privacy foram retirados do documento (Twitter, 2016a).

O tema Leis aplicáveis fica mais complexo a partir da versão 12, com aumento da regulação em países de atuação do Twitter. O endereço eletrônico https://support.Twitter.com/forms/privacy, que se encontra descontinuado em 2022, figurou à época como endereço para envio de dúvidas e comentários sobre o tema. O documento explicou que para ter acesso a contas e assistir *lives* via Periscope[23] o usuário não precisaria necessariamente ter um perfil na rede, porém, seus dados seriam coletados ainda que não subscrevesse a plataforma, com possibilidade de utilização por empresas de pesquisa e tendências de mercado (Twitter, 2016c).

Na PP 12 admitiu-se o envio de indicações via monitoramento de atividade do usuário até mesmo fora da plataforma. Seriam restritos conteúdos segmentados por raça, religião, política, vida sexual e saúde. O Twitter indicou que o direcionamento de anúncios poderia ser customizado pelo usuário em um link disponibilizado no PDF do documento.[24] Mensagens particulares poderiam ser visualizadas por demais usuários, caso o compartilhamento fosse de *posts* públicos. O Twitter aderiu ao UE-EUA Privacy

---

[23] O Periscope foi um app comprado pelo Twitter em 2015 por 100 milhões de dólares. Era utilizado para transmissão de lives na plataforma digital, mas teve sua utilização encerrada em 31 de março de 2021, sendo deixada a página apenas para leitura de transmissões feitas no passado. De acordo com a empresa, o app apresentava um alto custo de manutenção e deixou de ser viável financeiramente para a plataforma digital. Mais informações em: https://help.Twitter.com/pt/using-Twitter/periscope-faq Acessado em 30/06/2022.

[24] O endereço compartilhado via link clique aqui foi o https://business.Twitter.com/en/help/troubleshooting/how-Twitter-ads-work.html, que em 2022 segue informações em inglês.

Shield e um link foi estabelecido para que os usuários pudessem fazer reclamações (Twitter, 2016c).

A mudança na PP foi ocasionada pela adesão do Twitter ao European Commission´s Code of Conduct for Countering Illegal Hate Speech, que obrigou as plataformas digitais a se comprometerem com a mitigação de discursos de ódio na rede. Segundo o acordo, torna-se preciso dar aos usuários uma forma eficiente de denúncia para conteúdo xenófobo, racista e violento, com possibilidade de exclusão da mensagem no prazo de 24 horas após a notificação. Porém, a Lei deixou para as empresas a definição do que seria considerado impróprio. O excesso de discricionariedade das plataformas tornou a medida ineficaz no tratamento da propagação de violência na rede (Belli; Francisco; Zingales, 2017)

Disputas judiciais com relação a tratamento de dados seriam tratadas administrativamente, por meio de JAMS[25] ou ainda de arbitragem. De acordo com a PP 12, investigações e execuções estariam sujeitas à Comissão de Comércio Federal dos Estados Unidos. O Safe Harbor Principles of Privacy, referência de norma para o usuário europeu foi estabelecido em conformidade com o Privacy Shield. Endereços da empresa em São Francisco, na Califórnia, e em Dublin, na Irlanda, foram divulgados como centros para que os usuários mandassem suas dúvidas (Twitter, 2016c).

Poletto e De Moraes (2019) elencaram três paradigmas de controle propostos pelo Twitter depois de 2016. A partir deste período, ficariam banidos: conteúdo de terrorismo, exploração sexual de menores, abuso ou assédio, discursos de ódio, suicídio, automutilação, mídia sensível e finalidade ilegal; com relação à privacidade estavam restritos material sobre informações privadas e nudez não consensual; por fim, com relação à autenticidade a plataforma endereçou a proibição de spam, manipulação da plataforma, identidade falsa e apropriação de direitos autorais. A ação da plataforma de demarcações de temas atenderia demanda social, mas a execução da moderação mostrou-se comprometida pela remoção em massa de conteúdo, ocasionando cerceamento na liberdade de expressão, excessos na discricionariedade do moderador e controle do discurso público. Faltaram limites ao executor da tarefa,

[25] JAMS é um serviço global, independente e particular de resolução de conflitos fundado em 1979. De acordo com a empresa, cerca de 18.000 casos são resolvidos anualmente. Disponível em: https://www.jamsadr.com/about/ Acessado em 11/07/2022.

sem balizamento legal para julgamento do que seria ou não legítimo deletar. Análise compartilhada também por Keller (2020).

A 13ª versão da PP trouxe a opção de personalização dos anúncios[26] por conta da adesão do Twitter aos princípios de autorregulação da Digital Advertising Alliance (DAA). Foi indicado aos usuários que a personalização da plataforma inclui a interação com serviços de parceiros, cujos dados de navegação são compartilhados e agregados ou excluídos em 30 dias, dependendo da relevância. O usuário poderia fazer a configuração da coleta de dados em seus navegadores de internet para evitar que o Twitter fizesse o direcionamento de anúncios, perfis e conteúdo por inferência de comportamento na rede.[27] Dados de cartão de crédito, incluindo o código de segurança, passaram a ser compartilhados com empresas com as quais o usuário fizesse transações comerciais via plataforma, sem restrição alguma. O Safe Harbor saiu da versão 13, ficando apenas o Safety Shield, como instrumento de resolução de disputas sobre processamento de dados de EUA-UE e EUA e Suíça (Twitter, 2017a).

Uma drástica mudança de redação foi registrada entre as versões 13 e 14 da PP. A recomendação era de Leitura na íntegra do documento, que tiveram um incremento de complexidade. As instruções básicas foram redigidas em tópicos:

- O Twitter seria público e os tweets visíveis, formas de interação sob pseudônimo e comunicações diretas estariam disponíveis.
- Mesmo sem perfil na plataforma, os dados seriam coletados ao acessar o Twitter e o visitante poderia escolher se compartilhava informações adicionais como endereço de e-mail etc.
- Informações compartilhadas no Twitter poderiam ser checadas pelo usuário, assim como preferências de marketing e segurança da conta.
- Atividades na plataforma e dados pessoais poderiam influenciar a inferência da plataforma com relação ao perfil do usuário, estas informações estariam à disposição para checagem.
- A opinião do usuário sobre a PP foi pedida por meio de link.

Na 14ª versão da PP a plataforma admitiu que fornecia dados dos usuários mediante pagamento, inclusive para empresas que não eram parceiras da plataforma,

---

[26] O endereço da web https://Twitter.com/personalization foi deixado como opção aos usuários que quisessem fazer sua personalização de visualização de anúncios.

[27] O endereço https://Twitter.com/your_Twitter_data poderia ser utilizado para checar dados coletados utilizados para indicações por inferência de navegação.

mas que adquiriam as informações em larga escala para atividades comerciais. De acordo com o documento, o direcionamento de anúncios destas empresas talvez pudesse atingir usuários que já tivessem desativado em suas contas esta possibilidade, um endereço eletrônico foi disponibilizado para esta checagem.[28] O Periscope ficou disponível para acesso por contas do Twitter, Google ou Facebook. Uma outra seção foi feita em tópicos, trazendo detalhes sobre configurações de privacidade e segurança como: tweets disponíveis publicamente, configurações de marcação em fotos, mensagens diretas que poderia receber, disponibilidade do e-mail e número de celular para localização, divulgação de catálogo de endereços do Twitter, quando e onde acessar conteúdo confidencial e bloqueio ou silenciamento de contas (TWITTER, 2018a).

A localização do usuário passou a ser coletada a partir das configurações indicadas por ele em sua conta e dois links sobre estas informações foram deixados para checagem. A plataforma admitiu que usaria os dados coletados em navegadores de acesso aos *posts* do Twitter em páginas da web para, segundo sua interpretação: direcionar publicidade por interesse, personalizar experiência por dispositivo de acesso, usar informações de localização, personalizar experiência por GPS e monitorar navegação na web. A plataforma anunciou que coletaria informações de anunciantes e desenvolvedores, usuários de suas APIs (Twitter, 2018a).

Usuários da UE foram excluídos destas novas ações de tratamento de dados e ganharam um acesso exclusivo ao Data Protection Officer do Twitter. O processamento dos dados foi submetido a Leis vigentes nos países de origem do usuário e um link foi disponibilizado para checagem dos detalhes do Privacy Shield, acordo ao qual a plataforma já havia aderido no passado. Além disso, a plataforma abriu a possibilidade de portabilidade dos dados do usuário e *download* das informações coletadas (Twitter, 2018a).

A plataforma explicitou, na 15ª PP, que um único usuário poderia criar várias contas públicas para expressar seus diferentes posicionamentos e ideias. Também incentivou a interação do usuário com anúncios, para que o público-alvo pudesse ser mais bem compreendido pelo anunciante. O documento alertou que ao compartilhar um tweet, o usuário estaria indicando concordar com o conteúdo, sinalizando ao

[28] O endereço https://developer.Twitter.com foi disponibilizado para que o usuário checasse o direcionamento de anúncios de empresas que haviam comprado dados da plataforma.

Twitter para fazer o mesmo, aumentando sua distribuição (Twitter, 2020b). Dijck e Waal (2018) sinalizam, porém, que as plataformas digitais, inclusive o Twitter, não são neutras e a distribuição de conteúdo atende aos interesses comerciais, de atores governamentais e até mesmo exércitos de robôs que podem influenciar o alcance de determinados assuntos de forma artificial.

A autorização para marcação em fotos também foi incentivada, dizendo ao usuário que ele tinha sorte por um amigo lembrar-se dele. O escaneamento das mensagens diretas do usuário seria feito, de acordo com a plataforma, a pretexto de evitar spam. Além disso, o Twitter alertou que apesar de um usuário não poder retweetar uma mensagem direta, ele ainda poderia manter uma cópia da conversa (Twitter, 2020b).

Compartilhamento de informações de pagamento passaram a ter necessidade de anuência do usuário para processamento e checagem de fraudes. O Twitter detalhou que os dados coletados por atividade, direcionamento de anúncio e acesso aos serviços por terceiros poderiam ser combinados. De acordo com a versão 15 da PP, parceiros poderiam ter acesso a lista de mailing da plataforma para envio de anúncios. Conteúdo, que segundo a plataforma, seria contrário às normas do Twitter seriam retirados, como aqueles que glorificavam a violência, com notificação do usuário. Além disso, indicou que a mudança das configurações de privacidade feita pelo usuário poderia demorar um pouco para entrarem em ação (Twitter, 2020b).

Silva *et al.* (2019) notaram que Jack Dorsey, CEO do Twitter em 2018, chegou a publicar em sua conta na plataforma a inabilidade da rede em lidar com conteúdo abusivo, de assédio, ação de *trolls*,[29] campanhas de desinformação e um ecoar de mensagens de bolhas ideológicas. Como resposta, os usuários comentaram na publicação que gostariam de ver mais transparência sobre as infrações cometidas, não bastando colocar um algoritmo que apenas retirasse o *post* do ar. A rede admitiu ter uma quantidade enorme de conteúdo a ser moderado, transformando a tarefa num trabalho exaustivo. Houve até declarações públicas reconhecendo a utilização da rede para disseminação de conteúdo violento.

[29] Trolls foi um termo criado na internet para designar um usuário que desestabiliza uma conversa.

O Twitter chegou a assinar um termo de compromisso com a Anti-Defamation League (ADL) [30]para tentar reduzir campanhas difamatórias. A ADL, em parceria com a Stanford University, criou o Best Practice for Challenging Cyberhate (BPCC), fazendo considerações às redes sociais sobre as melhores formas de combate ao discurso de ódio nas redes sociais digitais. Notou-se, a partir destas recomendações, que algoritmos foram treinados para identificar textos e imagens ofensivas, porém, a ação era ineficaz, já que a máquina não substitui o componente humano. Moderadores terceirizados afirmaram à imprensa que chegavam a analisar 3500 mensagens por dia, sendo uma a cada oito segundos, não havendo espaço para análise, apenas para deletar o *post*, ou encaminhar às autoridades, o que ocorria em casos de pedofilia e suicídio (Silva *et al.*, 2019).

Uma pequena mudança foi adicionada à versão 16 da PP, retirando do texto quais informações não poderiam ser compartilhadas com parceiros comerciais e direcionando o usuário para checar as mudanças na Central de Ajuda da plataforma. Além disso, foi estabelecido que o controlador das informações para moradores da UE, países da Associação Europeia de Livre Comércio (EFTA) e Reino Unido seria a Twitter Internacional Company, baseada na Irlanda, para os demais o controle estaria a cargo da Twitter, Inc., sediada nos EUA (Twitter, 2020d).

A versão 17 da PP trouxe a possibilidade de utilização da rede para perfil profissional, com compartilhamento de dados como categoria profissional, endereço, e-mail e telefone e autorização no caso de administração de perfil de empresa. Ficou prevista a transcrição de material postado em áudio ou vídeo, com engajamento público destas postagens. O envio de pagamento em dinheiro, feito em transações dentro da plataforma, estariam sujeitos a monitoramento. A reprodução automática de vídeos, com coleta de dados sobre audiência, poderia ser modificada pelo usuário para impedir que o site originário do material recebesse as informações de visualização (Twitter, 2021a).

O Twitter informou, diferentemente do que foi descrito na PP 14, que não vendia dados dos usuários conforme definido no California Consumer Privacy Act (CCPA). A transferência de dados para processamento de usuário da UE, Brasil ou Reino Unido teriam uma segurança estabelecida em adequações legais de proteção que poderiam

[30] ADL é uma organização anti-ódio, que visa defender o tratamento justo aos povos judeus, fundada em 1913. Combate o antissemitismo, preconceito e extremismo contra os povos de origem judia. Busca garantir uma sociedade mais justa. Disponível em: https://www.adl.org/about-adl Acessado em 23/08/2022.

ser checadas por meio de cláusulas contratuais padrão para as quais foi destinado um link no PDF Twitter, 2021a). Já no início da PP 18, o Twitter trouxe uma reclamação, que soou como desabafo:

> É realmente difícil contentar a todos com uma Política de Privacidade. A maioria das pessoas que usam o Twitter querem algo curto e fácil de compreender. Embora desejemos poder encaixar tudo o que você precisa saber em um Tweet, nossos reguladores requerem que cumpramos nossas obrigações legais, descrevendo-as todas com muitos detalhes (Twitter, 2022d).

O documento disponibilizou links de acesso para maiores informações sobre coleta de dados, disponibilização de serviços de afiliadas e execução do tratamento de dados para personalização de serviço. Uma central de ajuda foi disponibilizada para esclarecimentos. O texto enfatizou que a redação da PP foi simplificada ao máximo para facilitar a compreensão dos leitores. A redação assumiu uma linguagem de conversação com o leitor, numa tentativa aparente da plataforma de simular uma relação de amizade com seus usuários, justificando o tempo todo o porquê da coleta de dados (Twitter, 2022d).

O Data Protection Office já não estava mais presente nesta versão e o documento informava que quem quisesse entrar em contato confidencial com o responsável pelo tratamento de dados pessoais do Twitter deveria fazê-lo via Formulário de Consulta de Proteção de Dados, cujo hiperlink estava disponível. O hiperlink remetia o leitor para uma página na qual um telefone, com horário de atendimento das 9h30 às 13h e das 14h às 17h30, de segunda à sexta, estava disponível (Twitter, 2022d).

5.1.2 Termos de Serviço

Em 2009, o Twitter deu início à publicação dos TS. O primeiro documento foi lançado sem uma data específica e dispunha de apenas três seções de instruções ao usuário: Termos Básicos, Condições Gerais e Direitos Autorais. Os Termos Básicos de utilização reafirmaram a idade mínima de 13 anos como condição para ter uma conta no Twitter, deixando o usuário responsável pelo conteúdo com o qual teria contato. Além disso, as regras impunham o não compartilhamento de conteúdo ilegal ou utilização da plataforma para condução de negócios ilícitos, atividade *hacker*[31],

[31] Atividade *hacker* é caracterizada pela invasão de dispositivos eletrônicos, redes e sistemas de computação, seja para verificar o sistema de segurança ou praticar crimes.

disseminação de vírus e criação de perfil falso. A plataforma informou que poderia remover, ou não, qualquer conteúdo que considerasse ilegal, ofensivo, ameaçador, difamatório, calunioso, obsceno ou que infringisse regras referentes a direito autoral (Twitter, 2009a).

Apesar de se autointitular um conduíte de conteúdo, desde o princípio o Twitter se mostrou um editor da produção de terceiros, admitindo a ação de moderação no primeiro TS. Mostrou-se um *gatekeeper* da informação, fazendo a curadoria ao usuário, porém, sem amparo legal ou legitimidade para exercer tal liberdade editorial. “O fato desperta indagações acerca dos limites da programação de seus algoritmos, de suas motivações editoriais e dos parâmetros de atividades de moderação que incidem no discurso de terceiros” (Pinheiro; Pinheiro, 2021, p. 590). Neste sentido, admitiu que não apenas fazia a mediação do discurso, mas o constituía a partir de mecanismos próprios de controle autorregulatório.

Gillespie (2018) indicou que o público só teve noção de quais eram os discursos proibidos quando documentos internos das plataformas digitais, enviados a moderadores terceirizados, foram vazados em 2012. Nos termos de serviço as informações foram superficialmente divulgadas, com a invocação de que o usuário usasse o bom senso para decidir o que postaria, porém, desde o princípio, as plataformas baseadas nos Estados Unidos estavam autorizadas para agir com liberalidade. A falta do arcabouço legal permitia que não fossem questionadas pela forma como lidavam com o conteúdo. E o que valia para os EUA era aplicado no restante do mundo.

Quanto ao material compartilhado, a plataforma deixou claro que qualquer extensão de arquivo postada era de inteira responsabilidade do usuário, que deveria atentar para a postagem de conteúdo aceitável, não descrevendo o que queria dizer com o termo “aceitável”. Os termos de serviços especificaram que era proibido o uso da plataforma para ameaçar, abusar ou assediar demais membros da comunidade. Estabeleceu a responsabilidade pela confecção de senha segura pelo usuário. Ao final do texto havia uma referência explicando que os termos de uso do Twitter haviam sido inspirados no documento emitido pela Flickr, que é um site de compartilhamento de imagens (fotografias, desenhos e ilustrações), com permissão da plataforma (Twitter, 2009a).

As Condições Gerais descritas no primeiro documento, informavam que os serviços da plataforma poderiam ser modificados ou interrompidos a qualquer

momento, sem aviso prévio ao usuário. O regramento alertava que a modificação dos termos de serviço seria feita a qualquer tempo, sob a discricionariedade da plataforma, de boa-fé, com base no senso comum e sensato julgamento, com a notificação ao usuário via e-mail ou qualquer outro canal escolhido por ele para esta comunicação. O usuário estava avisado que poderia ter seu acesso suspenso ou interrompido e que a plataforma julgaria a retirada do ar de conteúdo de acordo com sua compreensão de ilegalidade ou imoralidade. O Twitter sinalizou para a possibilidade de resgate de discussão sobre posse de nomes na plataforma e ainda a necessidade de reciprocidade de páginas que tivessem seus links compartilhados pelo usuário (Twitter, 2009a).

Os Direitos Autorais foram sinalizados neste termo de seção de serviços com o detalhamento de que qualquer conteúdo original postado pelo usuário teria seus direitos respeitados. Quando da saída de um usuário da plataforma, todo o conteúdo postado por ele seria retirado. Além disso, a plataforma detalhou como deveriam ser feitas as reclamações por uso indevido de conteúdo autoral, com garantia de retirada do ar de material comprovadamente postado em desrespeito à Lei de direitos autorais, subtende-se que o regramento utilizado seria o dos Estados Unidos (Twitter, 2009).

No dia 10 de setembro de 2009, uma segunda versão dos TS foi publicada, indicando maior complexidade das normas que foram distribuídas em 15 seções. O conteúdo foi classificado como qualquer informação postada, em todos os formatos (áudio, texto, vídeo ou gráfico). O regramento à época permitia à plataforma: direcionar publicidade, se eximir de qualquer responsabilização, se isentar de checagem quanto à veracidade de informações, disseminar mundialmente o post, isento de royalties, compartilhar com terceiros em qualquer mídia e via API, sem pagamento de recompensa financeira, com previsão de edição ou até modificação do conteúdo para melhorar a distribuição. O usuário seria responsável pelo conteúdo consumido e postado, pelos direitos autorais dos posts e de questionamentos judiciais de conteúdo, inclusive os compartilhados por terceiros (Twitter, 2009b).

Barbosa (2022) reflete que não só os usuários comuns, mas também as mídias alternativas, que encontraram na internet o ambiente ideal para o exercício do jornalismo independente, encontram grande dificuldade de entender a lógica dos algoritmos de distribuição de conteúdo. Isso porque as regras são opacas e há uma série de questionamentos sobre a propagação de conteúdo extremista que notadamente é mais disseminado devido ao maior número de cliques que gera. Além

disso, a produção de conteúdo profissional alimenta o engajamento das plataformas e a monetização é outro tema que se encontra regulado de forma genérica dentro dos TS das plataformas.

Com relação aos termos de privacidade e segurança, o documento previu que o Twitter iria coletar, armazenar e processar os dados do usuário. Deixou claro que estes dados poderiam ser compartilhados com empresas parceiras. O TS ainda indicou o compartilhamento das informações com governos em investigações que solicitassem dados, sob escrutínio da Lei aplicável e devidamente referendada. A versão 2 trouxe o endereço eletrônico Twitter.com/tos para conferência das mudanças nos TS em versões mais atualizadas (Twitter, 2009b).

Apenas oito dias após a divulgação da versão 2, o Twitter publicou a terceira atualização dos TS. Notadamente, o que foi promovido de mudança ficou evidenciado na indicação de questões chave, intituladas Tips (Twitter, 2009c). Ao todo foram adicionadas sete frases, quatro traziam indicações sobre moderação de conteúdo, privacidade e segurança:

- Esta licença nos autoriza a mostrar o seu tweet para o resto do mundo e que outros façam o mesmo. Mas o que é seu é seu – você é dono do seu conteúdo.
- O Twitter tem um conjunto de regras em evolução sobre como os desenvolvedores de API podem interagir com o seu conteúdo. Essas regras existem para permitir um ecossistema aberto com seus direitos em mente.
- A API do Twitter existe para permitir e encorajar a reutilização de conteúdo.
- O Twitter não divulga informações de identificação pessoal a terceiros, exceto de acordo com nossa política de privacidade

Para Gillespie (2022) a ação relacionada ao conteúdo passa por duas vias, a moderação e a recomendação. A primeira suprime, retira do ar conteúdo e a segunda oferece material. A retirada do ar implica em saber quais mensagens são permitidas e na recomendação quais vozes ou discursos serão privilegiados. Nas mídias tradicionais isso é feito usualmente, dando voz a figuras centrais e deixando minorias de fora das páginas de jornais, revistas e telejornais. Era fácil identificar o que era publicidade e o que poderia ser classificado como notícia, opinião, cada assunto tinha um espaço definido. Porém, nas redes sociais digitais estas regras são mais nebulosas e os usuários têm dificuldade de identificar estas diferenças.

No documento da quarta versão dos TS, publicado no final do ano de 2010, foi adicionado que nenhuma outra empresa, além daquelas controladas pelo Twitter,

seriam beneficiadas pelas normas autorregulatórias (Twitter, 2010c). Na versão 5 o TS apenas modificou uma informação, ao invés de informar o compartilhamento de informações com desenvolvedores, a plataforma substitui o termo por parceiros, que poderiam oferecer qualquer tipo de produto ou serviço. O documento acrescentou ainda que as fotos do usuário seriam parte de seu conteúdo (Twitter, 2011a).

No início da sexta versão dos TS a plataforma especifica os serviços aos quais o documento estava submetido que incluíam o endereço na web, SMS, APIs, notificações por e-mail, aplicativos, botões e widgets. Foi estabelecida a necessidade de autorização para aceitação dos termos em nome de uma companhia, organização, governo ou cliente. Além disso, o documento acrescentou que o usuário deveria concordar com a proposta do Twitter de fornecer, promover e melhorar os serviços em ordem de disponibilizar o conteúdo às empresas parceiras da plataforma, pelos seus canais (Twitter, 2012b).

Em lugar de autorização para retransmissão de conteúdo, a versão 6 especificou que a autorização incluía a possibilidade de as empresas parceiras transmitirem, distribuir ou publicar o conteúdo, com toda a responsabilização legal advinda da ação a cargo do usuário. E tudo isso apresentado de forma que o usuário compreendesse a possibilidade de utilizar a plataforma como um grande benefício:

> O Twitter oferece a você uma licença pessoal, mundial, isenta de royalties, intransferível e não exclusiva para usar o software fornecido a você pelo Twitter como parte dos serviços. Esta licença tem o único propósito de permitir que você use e aproveite os benefícios dos serviços fornecidos pelo Twitter, da maneira permitida por estes termos (Twitter, 2012b).

Ficou prevista a suspensão da conta, além da exclusão que já havia sido aventada, com indicação de esclarecimentos via endereço eletrônico.[32] Com relação aos direitos autorais, a retirada do ar de conteúdo denunciado ficaria sob a discricionariedade do Twitter, inicialmente sem risco ao autor. Nesta versão foi especificado que o usuário poderia desativar sua conta ou descontinuar a utilização, situação em que o perfil seria desativado por inatividade. Além disso, a plataforma especificou que poderia deixar de fornecer o serviço em algumas situações como: violação de termos de uso; criação de riscos legais para a plataforma; e inviabilidade econômica de prestação do serviço (Twitter, 2012b).

---

[32] Endereço para esclarecimentos sobre possibilidades para suspensão e exclusão de contas dev.Twitter.com

O Twitter informou que normas autorregulatórias não seriam aplicáveis em locais onde as Leis regressem à forma de operação da plataforma. Porém, manteve no documento a isenção de responsabilidade por precisão, integridade, disponibilidade, segurança ou confiabilidade de conteúdo; dano a equipamentos em acesso a links externos; exclusão ou falha no armazenamento ou disponibilização de mensagens; disponibilidade de serviços sem erros e ainda adicionou que a plataforma não teria qualquer comprometimento por queda na receita de empresas em consequência de postagens. Estabeleceu, no entanto, o valor máximo de US$ 100 ou o que o usuário paga pelo serviço, que é 0, para as reivindicações de danos causados, com discussões jurídicas previstas para EUA, com base no arcabouço legal da Califórnia (Twitter, 2012b).

De acordo com Alnajafi (2021), a intenção do Twitter provavelmente foi desincentivar a busca por resolução jurídica para descontentamento com a plataforma. Em cinco diferentes partes dos TS, que guardam a segurança jurídica da plataforma, é mencionado que ao ultrapassar o código moral do serviço, o usuário poderá sofrer sanções. Amato *et al.* (2022) observaram que em 2012, quando esta versão dos TS estava em vigência, o Tribunal Superior Eleitoral (TSE) do Brasil considerou irregular a utilização do Twitter para fazer campanha eleitoral fora do período pela justiça eleitoral brasileira. No ano seguinte, porém, compreendeu que pronunciamentos feitos em rede social fechada não configuraram campanha eleitoral extemporânea. Isso porque o TSE entendeu que o conteúdo seria restrito ao usuário que subscrevesse a página do pretenso candidato. Já em 2018, em 58,9% das ações propostas à justiça eleitoral, referente a conteúdo, as empresas de tecnologia – Facebook/WhatsApp, Google e Twitter – figuravam como réus no processo por disseminação de informações inverídicas.

O TS 7 esclareceu que a tradução para o português era uma ação para a conveniência do usuário, porém, apenas a versão em inglês seria válida para discussão de conflitos de interesse. A nova redação especificou que o usuário seria responsável não só pela publicação, mas também pela submissão, reprodução e disponibilização de conteúdo. O Twitter reiterou que não endossava opiniões transmitidas pelos usuários e instituiu a possibilidade de distribuição do conteúdo também via publicidade e por radiodifusão. Foi informada a facilitação no fornecimento de dados por pedido de entidade administrativa e não só governamental (Twitter, 2012c).

A versão 8 instituiu que conteúdo seria qualquer material postado pelo usuário, tanto que a dica mudou de “Você é o que você Tweettar”, para “Você é o que você divulga no Tweet”. A plataforma reconheceu que o usuário poderia não ser o dono do conteúdo que divulgava e transferiu a responsabilidade por danos a terceiros, caso o material compartilhado fosse ilícito ou danoso. A função Compre Agora, que exigiria informações de cartões de crédito de terceiros, instituiu a necessidade de aceitação dos termos comerciais da plataforma (Twitter, 2014b).

A versão 8 da PP nada trouxe sobre conteúdo agressivo ou violento, justo em 2014, quando a plataforma foi extremamente criticada por permitir perseguição à comunidade LGBTQIA+ e às mulheres. Um caso emblemático foi a campanha sexista postada utilizando como indexador a hashtag #Gamergate. A campanha teve início com a perseguição a uma desenvolvedora de games, Zoe Quinn, acusada pelo ex-namorado de receber boas críticas de seus jogos por manter um caso com um jornalista, crítico de games. A campanha difamatória envolveu programadores, jogadores e foi parar no New York Times (Gillespie, 2018).

Neste contexto, de falas inflamadas, vazou à imprensa uma declaração do CEO do Twitter à época, Dick Costolo, na qual ele afirmava que “chutaria” para fora da plataforma os agressores. Meses depois, o porta-voz da empresa, Vitaya Gadde, informou que o Twitter tentaria encontrar uma fórmula saudável entre liberdade de expressão e segurança do usuário (Gillespie, 2018).

A versão 9 dos TS retirou a possibilidade de compartilhamento de dados por interpelação administrativa e instituiu a necessidade de cumprimento de pré-requisitos e pedido formulado para reclamação sobre uso indevido de material com direito autoral. O documento ainda assinalou que o Twitter poderia acessar, ler ou preservar a divulgação de informações que visassem cumprir “legislação aplicável, regulamento, decisão judicial ou pedido de autoridade governamental” (Twitter, 2015b). As modificações que deram origem ao documento de número 10 do TS foram apenas de nomenclaturas de seções, sem alteração de normas (Twitter, 2016b).

Uma questão que poderia ter constado do documentou seria o combate ao terrorismo. Em 2016, o ISIS[33] publicou uma série de vídeos no Youtube, com decapitações de civis e jornalistas. Os vídeos foram compartilhados no Twitter e

[33] ISIS é o acrônimo de Islamic State of Iraq and Syria, um grupo terrorista com base no Oriente Médio que praticou atos terroristas em várias partes do mundo.

Facebook, gerando críticas e pedidos de retirada de conteúdo. Enquanto nos EUA famílias processavam Facebook e Twitter, sem conseguir vencer as ações, na Europa as plataformas digitais foram obrigadas a atender ao UK Terrorism Act de 2006, que obrigava a retirada imediata de conteúdo terrorista após aviso, sob pena de multa por apologia (Gillespie, 2018).

A versão 11 teve mudanças significativas na redação e complexidade de informações, porém, algumas instruções foram suprimidas e alocadas fora do documento principal, com acesso disponibilizado via links externos. No cabeçalho da página um aviso informava aos usuários de fora dos EUA, que TS, PP e Regras do Twitter eram políticas incorporadas à utilização da plataforma. Houve uma ênfase à informação de que o acesso aos serviços do Twitter dependeria da concordância integral com as normas do contrato e em caso da administração de conta corporativa era necessário ter autorização para esta ação (Twitter, 2016d).

A complexidade na forma com que as regras autorregulatórias foram apresentadas ao público ao longo do tempo deram margem a interpretações equivocadas, já que era difícil para a audiência acompanhar as mudanças e interpretar as regras de forma acessível. Um questionário aplicado nos EUA, em 2016, demonstrou que a maioria dos usuários achava que seus conteúdos haviam sido retirados do ar por ação humana: algum colega o denunciara à plataforma; ou, sua publicação havia recebido uma *flag* de um desafeto, que discordava de seu ponto de vista. Em menor número, outro grupo de usuários acreditava que a remoção de *posts* era ação de uma comunidade discordante. Por fim, uma outra parcela entendia que a moderação fazia parte do viés político do Twitter, que queria influenciar a campanha presidencial do país por meio de censura de conteúdo (Myers West, 2018).

As experiências pessoais com a moderação de conteúdo fizeram com que muitos usuários criassem conceitos próprios sobre a ação. A pesquisa de Myers West (2018) ilustrou a frustração de usuários com as mensagens e interfaces confusas da plataforma digital. A remoção de *posts* em massa e a dificuldade de entrar em contato com um funcionário que pudesse explicar em que ponto o usuário havia errado abriram espaço para a criação de explicações fantasiosas, como as citadas no parágrafo anterior, sobre a moderação de conteúdo.

Enquanto isso, a plataforma abria ainda mais margem à imaginação dos usuários, porque várias informações sobre a utilização dos serviços foi recebendo

endereços adjacentes aos documentos que dispunham sobre a oferta do serviço.[34] A plataforma reiterou que os TS permitiam o uso do conteúdo do usuário pelo Twitter, suas subsidiárias e parceiros, sem remuneração e que os direitos autorais deveriam atender normas estadunidenses e de outros países. Foi retirada a possibilidade de responsabilização do Twitter, com pagamento de qualquer quantia ao usuário lesado, prevista até a versão 10. O foro para discussões judiciais também desapareceu nesta versão e o endereço da empresa foi transferido da Califórnia, nos Estados Unidos, para Dublin, na Irlanda (Twitter, 2016d).

Nos TS ficaram concentradas as informações legais, como os usuários poderiam ser penalizados em face a descumprimento de normas da companhia. Fora do documento principal ficaram os códigos de conduta, com uma extensa discricionariedade para a plataforma classificar o que não se encaixaria no que a plataforma acredita como normas morais de comportamento. Não há uma definição exata do que a plataforma entende como Glorificação da Violência, ou Discurso de Ódio, por exemplo. O conceito dos termos está aberto a interpretações, o que deixa o usuário diante do poder de classificação da plataforma (Alnajafi, 2021).

Para a versão 12 dos TS pesou a remoção de conteúdo não só por infringir o DMCA, que trata dos direitos autorais, mas também de contas falsas, com material ilícito ou posts que configurassem assédio. O documento introduziu a possibilidade de reclamação do usuário, em caso de exclusão de conta. Com o aumento de normas regulatórias, o Twitter alertou sua aderência às Leis locais de cada país e atestou que informaria o usuário sobre mudanças de políticas que afetassem direitos e obrigações com 30 dias de antecedência (Twitter, 2017b). As punições variavam de 12 horas a sete dias e em tese, usuários que receberam algum tipo de sanção não poderiam criar outras contas, porém, na prática isso não ocorre (Jiménez Durán, 2022).

O que os estudiosos vêm observando desde os anos 2000 é que as regras para retirada de conteúdo do ar aplicadas pelas plataformas digitais são erráticas e discutíveis. Além disso, pouco claras ao público. O que é possível mensurar e quantificar são as retiradas por imposição legal, e ainda assim, nota-se uma remoção de conteúdo que excede o arcabouço legal disponível. Muitas vezes, a partir de uma

---

[34] Para a PP foi deixado o endereço Twitter.com/privacy. Artigos de esclarecimentos poderiam ser encontrados em https:support.Twitter.com/articles/15795 e para denúncias referentes à violação de direitos autorais, o formulário para detalhamento sobre o caso poderia ser encontrado em https:support.Twitter.com/forms/dmca

reclamação, a plataforma prefere remover o conteúdo, não sendo possível observar se por excesso de zelo, ou incapacidade de lidar com a questão (Keller, 2020a).

O Twitter seguiu a tônica de simplificação das regras na versão 13 dos TS, porém, foram adicionados novos endereços eletrônicos para comportar as informações retiradas do documento principal.[35] Na redação da peça foi especificado que as informações constantes do documento serviriam para usuários da União Europeia e outros países, com exceção de Estados Unidos (Twitter, 2018b). Van Dijck (2022) faz a ressalva de quando se observa como os Estados Unidos lidam com dados pode-se observar o foco centrado no mercado. Já quando se coloca a China em perspectiva neste sentido, o centralizador dos dados é o Estado. O quadro da União Europeia sinaliza com a possibilidade de uma via alternativa, entre benefícios para o mercado, sem esquecer o bem público. Porém, com respeito à privacidade do cidadão, que ficou marcada pelo RGPD de 2018.

Talvez por isso, houvesse por parte do Twitter uma preocupação de fatiar a discussão pensando em áreas de ação. Já com relação à idade para utilizar a plataforma, o TS 13 trouxe a idade mínima de 16 anos para experimentação com o Periscope, app utilizado para transmissão de *lives.* Para usuários que administravam contas comerciais, o Twitter trouxe maiores especificações a respeito de condições para utilizar os serviços, incluindo, além de direitos e poderes de postar conteúdo, também licenças, consentimentos e permissões (Twitter, 2018b).

A apropriação indébita de propriedade intelectual no uso de conteúdo de terceiros foi listada como infração de usuário na versão 14 dos TS. Foram previstas as ações de curadoria, transformação e tradução de conteúdo do usuário para melhor distribuição. O documento especificou que o acesso gratuito à plataforma daria ao Twitter o direito de utilizar o conteúdo do usuário também sem pagar (Twitter, 2020c). Para Belli (2019), o acesso sem custo é uma armadilha feita pelas plataformas de mídias sociais, especialmente o Twitter, Facebook e WhatsApp. A falta de concorrência no setor expõe a população a poucas opções de obter informação ou se relacionar online, mantendo estas plataformas como monopólios da arena pública moderna.

O problema da falta de opção deve persistir, segundo Van Dijck (2022): apenas 30% dos usuários estão dispostos a pagar por serviços como do Twitter, para evitar

35 Para termos de uso https://Twitter.com/pt/tos para PP https://Twitter.com/privacy

que seus dados sejam coletados. Com isso, Gillespie (2021) enfatiza que a moderação do discurso público segue conforme as ferramentas da plataforma que regula a distribuição das mensagens, prevendo em alguns casos impulsionamento, em outras silenciamento, exclusão, banimento, passando ainda por etiquetagem, num trabalho extenso de modificação que permite ou inibe a distribuição. Em todo este trabalho de moderação existe o usuário, que quer compreender o que lhe é mostrado, e o produtor de conteúdo, que necessita identificar quais assuntos são permitidos ou não na plataforma. A moderação de conteúdo tem dado às plataformas o poder de decidir quais mensagens são ou não permitidas no ciberespaço, que é público.

Voltou a figurar na redação a possibilidade de ressarcimento por danos causados ao utilizar o serviço até o valor de US$ 100. Para os moradores da UE o texto especificou que o controlador dos dados voltada a ser a sede em Dublin, com responsabilizações segundo Leis daquele território. Para os demais usuários o controlador dos dados voltava a ser a Twitter, Inc., em São Francisco, CA, com disputas judiciais de acordo com as Leis locais (Twitter, 2020c).

Ainda em 2020, a versão 15 dos termos de uso foi publicada, com nova simplificação sobre a oferta de serviços. Foi instituído que pesquisadores da área de segurança seriam obrigados a cumprir regras do Programa de Relatórios de Vulnerabilidades do Twitter com especificações constantes em uma página da web[36] (Twitter, 2020e). Na versão seguinte o Twitter voltou a especificar quais eram os serviços disponibilizados pela plataforma e suas afiliadas. Além disso, trouxe a possibilidade de cobrança de taxas por utilização de serviços ou recursos. Foi retirado desta versão o endereço para denúncias de direitos autorais para os serviços do Periscope. Desde 31 março de 2021, o app foi descontinuado pela plataforma digital, mas a página com o arquivo do conteúdo foi mantida (Twitter, 2021b).

A versão 17 trocou o termo falsidade ideológica por falsa identidade. A norma previu que a personificação de outras pessoas violava os TS. Foi prevista também a proibição pela tentativa de contorno das limitações técnicas da plataforma. Serviços pagos teriam regramento próprio que deveria ser observado pelos usuários. Moradores do Reino Unido foram novamente incluídos nas regras para contrato firmado com a afiliada do Twitter na Irlanda, assim como membros da União Europeia,

36 https://hackerone.com/Twitter

enquanto usuários do restante do mundo foram mantidos sob a tutela da Twitter, Inc., na Califórnia (Twitter, 2022e).

Para ajudar na visualização das mudanças propostas a cada nova versão dos termos de serviço do Twitter, elaboramos um resumo que traz as principais alterações a cada versão nos pontos de análise propostos por esta tese, que são moderação de conteúdo, privacidade e segurança do usuário. O detalhamento pode ser visto no Quadro 7.

Quadro 7 – Resumo das alterações nas versões da PP e dos TS do Twitter

Versão	Normas autorregulatórias de moderação de conteúdo	Normas autorregulatórias sobre privacidade do usuário	Normas autorregulatórias de segurança do usuário
PP– 2007	Inexistente neste documento de informações sobre a moderação do conteúdo	1) Uso de cookies 2) Uso de Log Data 3) Direcionamento de ofertas e publicidade 4) Processamento de dados 5) Compartilhamento de dados com terceiros	1) Previsão de monitoramento de atividade ilegal, antiética ou insegura na plataforma 2) Uso de criptografia para assegurar confidencialidade de dados para atores que não mantêm relacionamento com a empresa 3) Previsão de uso da plataforma para indivíduos acima de 13 anos de idade 4) Compartilhamento de dados com governos e autoridades policiais em casos de investigações

PP2 e TS 1 + TS 2 + TS 3 – 2009	1) Possibilidade de remoção de conteúdo considerado ilegal, ofensivo, ameaçador, difamatório, calunioso, obsceno ou que ofendesse direitos autorais (TS1) 2) Classificação de conteúdo como informação postada em todos os tipos de formato (áudio, texto, vídeo ou gráfico) (TS2) 3) Direcionamento de publicidade, compartilhamento do conteúdo do usuário mundialmente (TS2) 4) Reutilização de conteúdo (TS3)	1) Previsão de tratamento de dados (coleta, processamento e armazenamento) em qualquer país de operação da plataforma (PP2) 2) Previsão de informações públicas (bio, endereço e foto de identificação) (PP2) 3) Possibilidade de visualização da atividade do usuário na rede (curtidas, compartilhamentos, retweet) (PP2) 4) Exposição à política de privacidade de terceiros em caso de acesso via plataforma parceira, como Google (PP2) 5) Transferência de dados para empresa adquirente, em caso de venda do Twitter (PP2) 6) Remoção de usuários menores de 13 anos, denunciados por pais ou responsáveis (PP2); 7) Remoção de usuário que enviasse spam aos demais membros da comunidade (TS1) 8) Uso dos dados do usuário e compartilhamento das informações com o governo (TS2) 9) Usuário poderia bloquear o recebimento de comunicados do Twitter (TS2)	1) Proibição de negócios ilícitos, atividade *hacker*, disseminação de vírus e criação de perfil falso (TS1) 2) Possibilidade de suspensão ou interrupção de acesso sob a discricionaridade da plataforma, por suspeita de atividade ilegal ou imoral na utilização dos serviços (TS1) 3) Previsão de denúncia por utilização de material sob proteção de direitos autorais (TS1) 4) Compartilhamento dos dados para investigações de qualquer natureza (TS2) 5) Responsabilização do usuário por qualquer conteúdo postado, até mesmo quando modificado por terceiros (TS2)
PP 3, PP 4 e TS 4 – 2010	Sem modificações	1) Possibilidade de monitoramento das atividades relacionadas a cliques em link na plataforma (PP3) 2) Previsão de compartilhamento do IP da máquina do usuário e instalação de *cookies* por parceiros (PP3) 4) Monitoramento da navegação do usuário no Twitter e nos sites de parceiros (PP4) 3) Todas as empresas controladas pelo Twitter teriam acesso aos termos e dados do usuário (TS4)	Sem modificações

PP 5 e TS 5 – 2011	1) Além de desenvolvedores de API, parceiros comerciais poderiam interagir com conteúdo do usuário (TS5)	1) Monitoramento de dados por compartilhamento de tweets via SMS, adição de widget, sites pessoais, app de celulares (PP5)	Sem modificações
PP 6, TS 6 e TS 7– 2012	1) Indicação de conteúdo via monitoramento de dados, que poderia ser desativado via extensão de navegador da internet, em ferramenta nomeada de Do-Not-Track (PP6) 2) Permissão de transmissão, radiodifusão, distribuição e até publicação do conteúdo do usuário (TS6) 3) Twitter assumiu pagar até US$ 100 por danos ocasionados pelo acesso não autorizado e ainda o uso ou alteração de conteúdo (TS6) 4) Twitter reforçou que não endossa opiniões de usuários (TS6) 5) Possibilidade de remoção de conteúdo considerado inapropriado (TS6) 6) Possibilidade de distribuição do conteúdo do usuário via publicidade e radiodifusão (TS7)	1) Detalhamento da coleta de dados via Log Data que captação dados de operadora de celular e uso de apps móveis (PP6) 2) Possibilidade de recomendação de perfis para seguir (PP6) 3)Usuários representantes de contas comerciais precisam ter autorização para aceitar os termos de serviço (TS7) 4) Possibilidade de fornecimento de dados dos usuários por pedido administrativo e não somente governamental (TS7)	1) Adesão ao Safe Harbor UE – que impõe parâmetros para segurança, integridade de dados, acesso, avisos e escolhas (PP6) 2) O Twitter se eximiu de responsabilidade por: a) Dano a equipamento do usuário ocorrido no acesso a conteúdo danoso b) Falha de armazenamento c) Erro na disponibilidade do serviço da plataforma d) Perda de ganhos ou receitas e) Estabeleceu a corte de São Francisco (CA) para reclamações judiciais 3) Remoção de contas por: inatividade; violação dos TS; criação de riscos legais e inviabilidade econômica da plataforma (TS6)
PP 7 e P– 8 - 2013	Sem modificações	1) Customização de anúncios via *cookies* de navegação do usuário em sites parceiros, com possibilidade de retirada do monitoramento (PP7) 2) Ficou previsto que se identificado o compartilhamento de dados de menores de 13 anos, estas informações seriam excluídas (PP7) 3) Monitoramento de interação do usuário em anúncios (PP8) 4) Previsão de uso de outros sistemas de monitoramento além de *cookies* (PP8)	1) Foi esclarecido que contas desativadas ficariam 30 dias aguardando pedido de recuperação (PP7)

PP 9 e TS 8 – 2014	1) O conceito de conteúdo evolui de material postado para compartilhado (TS8) 2) Reconhecimento de que o usuário poderia não ser o dono do conteúdo compartilhado (TS8)	1) Disponibilização de dados para pesquisas acadêmicas, de tendências e percepções, inclusive de agências de saúde (PP9) 2) Monitoramento de Apps baixados via Twitter (PP9) 3) Novas regras são impostas para a captação de informações de terceiros em contas comerciais (TS8) **** estas regras foram postadas fora dos termos de serviço em páginas adjacentes*	1) Guarda de informações de cartão de crédito com exceção do CVV e endereço de entrega da compra (PP9) 2) Compartilhamento de todas as informações com os parceiros envolvidos na transação comercial (PP9) 3) Usuários comerciais foram citados, porém sem especificações sobre utilização dos dados compartilhados (TS8) 4) Responsabilização do usuário por acesso de terceiros a conteúdo ilícito ou danoso postado por ele (TS8)
PP10 e TS 9 – 2015	1) Mudança de conceito, o tweet passa de um dizer para uma divulgação (PP10) 2) Admissão de direcionamento de conteúdo com base em tweets e retweets (PP10) 3) Especifica como fazer reclamação sobre uso indevido de conteúdo original (direitos autorais na forma do DMCA) (TS9)	1) Envio de notificações do Twitter via serviços de terceiros utilizados pelo usuário (PP10) 2) Inclui concordância para a transferência e processamento dos dados do usuário para Estados Unidos e Irlanda (TS9) 3) Retirada da possibilidade de compartilhamento dos dados do usuário por interpelação administrativa (TS9)	1) A administradora dos dados se divide: usuários dos EUA ficam sob a tutela da Twitter Inc., os demais passam para Twitter Internacional Company, da Irlanda (PP10) 2) Previsão expressa da possibilidade de uso de pseudônimo em conta (PP10) 3) Possibilidade de divulgação de tweets antigos, por terceiros, mesmo depois que uma conta fosse excluída (PP10) 4) Decisão discricionária do Twitter de acessar, ler ou compartilhar informações do usuário para cumprir decisão judicial ou governamental (TS9) 5) Pedidos de checagem de direitos autorais ganham especificações (TS9)

PP 11, PP 12, TS 10 e TS 11– 2016	1) Alerta para verificação do conteúdo a ser postado de acordo com as normas dos TS (PP11) 2) Direcionamento de conteúdo de anúncios com base em atividade externa à plataforma (PP12) 3) Restrição de segmentação de conteúdo por raça, religião, política, vida sexual e saúde (PP12) 4) Alerta ao usuário para checagem de segurança de conteúdos postados (TS11)	1) Previsão da coleta de dados de usuários do Periscope, mesmo que não subscritos aos Twitter (PP12) 2) Previsão de compartilhamento dos dados de usuários com empresas particulares de pesquisa de tendências de mercado (PP12) 3) Exposição de atividades de curtidas compartilhadas de forma privada (PP12) 4) Simplificação das informações e alocação do inteiro teor da política de privacidade em endereço externo (TS11) 5) Administração de contas corporativas ou governamentais apenas com autorização específica (TS11)	1) Retira do documento a adesão ao Safe Harbor Principles of Privacy (PP11) 2) Adesão da plataforma ao EU-EUA Privacy Shield (PP12) 3) Uso de JAM e arbitragem para resolução de conflitos (PP12) 4) Sujeição de documentos, investigações e execuções à Comissão de Comércio dos EUA (PP12) 5) Retorna ao documento a adesão ao Safe Harbor Principles of Privacy (PP12) 6) Retira a possibilidade de o Twitter ser responsabilizado e pagar até US$ 100 por danos ocasionados pelo acesso não autorizado e ainda o uso ou alteração de conteúdo (TS11) 7) Retira-se a possibilidade de discussões judiciais nos EUA e transfere-se o endereço da empresa para Dublin, Irlanda (TS11) 8) Impôs regras e responsabilidades para usuários de serviços comerciais da plataforma como Twitter para Sites, Cartões do Twitter, Desenvolvedor e Termos de comércio (TS11) **** estas regras foram postadas fora dos termos de serviço em páginas adjacentes*

PP 13 e TS 12 – 2017	1) Possibilidade de personalização de exposição a conteúdo de anúncios (PP13) 2) Indicação de conteúdo via monitoramento de acesso por navegador (PP13) 3) Instituiu que a remoção de conteúdo pode se dar não só por direitos autorais, mas também por identificação de postagem por contas falsas, material ilícito ou configuração de assédio (TS12)	1) Retirada do documento de informações sobre coleta de dados via widget (PP13) 2) Monitoramento de acesso à plataforma via navegador (PP13) 3) Possibilidade de checagem de direcionamento de anúncios por inferência (PP13) 3) Estabeleceu prazo de 30 dias para aviso aos usuários sobre mudanças significativas nos TS que afetassem direitos e obrigações (TS12)	1) Anúncio de adesão à Digital Advertising Alliance (DAA) (PP13) 2) Compartilhamento de todas as informações referentes a transações comerciais (PP13) 3) A adesão ao Safe Harbor deixa novamente a redação, mencionando apenas o Safety Shield como instrumento de resolução de conflitos (PP13) 4) Ofereceu um endereço eletrônico para reclamação por remoção de conta (TS12) 5) Citou que Leis locais seriam as balizas para responsabilização da plataforma, funcionários e empresas parceiras (TS12)
PP 14 e TS 13 – 2018	1) Possibilidade de direcionamento de conteúdo de anúncios, mesmo que desativada a ação, porque algumas empresas compravam dados do usuário (PP14) 2) Admissão de que o Twitter direciona e customiza conteúdo por meio de consumo do usuário aos posts da plataforma (PP14) 3) Direcionamento de conteúdo via monitoramento de localização por GPS (PP14) 4) Especificou-se que áudios também são conteúdo sujeito às mesmas regras de material postado pelo usuário na plataforma em qualquer outro formato (TS13) 5) Instituiu a necessidade de administradores de contas comerciais terem licenças, consentimentos e permissões para postagem de conteúdo em nome da marca que representam (TS13)	1) A plataforma pediu a opinião do usuário sobre a PP (PP14) 2) Admitiu o fornecimento dos dados do usuário mediante pagamento (PP14) 3) Monitoramento dos dados dos anunciantes via Twitter Ads (PP14) 4) Monitoramento de experiência de acesso por suporte (PP14) 5) Instituiu o mínimo de 16 anos para utilização do Periscope, APP utilizado para *lives* (TS13) **** as regras específicas para utilização do APP foram postadas fora dos termos de serviço em páginas adjacentes*	1) Possibilidade de customização de configurações de visualização e segurança – como bloqueio e silenciamento de contas (PP14) 2) Possibilidade de bloqueio de direcionamento de anúncios por interesse, de acordo com a DAA (PP14) 3) Abertura do Data Protection Officer para usuário EUA - UE (PP14) 4) Possibilidade de download e portabilidade dos dados (PP4) 5) Oferta de link para checagem dos usuários quais seriam as Leis vigentes em seus países sobre a proteção de dados (PP14)

PP 15, PP 16, TS 14, e TS 15 - 2020	1) Alerta ao usuário que o retweet indicava concordância do usuário com o conteúdo do post, dando anuência para maior distribuição da mensagem (PP15) 2) Possibilidade de retirada de conteúdo em desacordo com as políticas da plataforma, como glorificação à violência, sem detalhamento expresso da conduta (PP15) 3) Admitiu a curadoria do conteúdo com transformação e até tradução para aumentar a distribuição (TS14) 4) Possibilidade de restringir distribuição e limitar a visualização de posts (TS14)	1) Possibilidade de exclusão de usuário mediante pedido, pós checagem de informações da plataforma (PP15) 2) Com exceção dos usuários do bloco comum europeu, os demais espalhados pelo mundo, foram colocados em igualdade de direitos e obrigações no uso da plataforma (TS14) 3) Foi confirmado, porém, foro diferenciado para dirimir atritos entre moradores da União Europeia e a plataforma (TS14)	1) Admissão pública de que usuários poderiam ter diversas contas, para expressar linhas de pensamento diferentes (PP15) 2) Previsão de anuência do usuário para compartilhamento de informações comerciais em transações financeiras (PP15) 3) Usuário de fora da UE, EFTA e Reino Unido voltaram a ter seus dados sujeitos à Twitter Inc, dos EUA (PP15) 4) Instituiu a figura de responsabilização por apropriação indébita de propriedade intelectual no uso de conteúdo de terceiros (TS14) 5) Retornou ao texto a possibilidade de ressarcir usuários pelo acesso ou uso indevido de conteúdo em US$ 100 (TS14) 6) O foro da Califórnia retorna como base para discussões judiciais fora da União Europeia, enquanto os usuários desta localidade ficaram sob a tutela da justiça irlandesa (TS14) 7) Instituiu que pesquisadores da área de segurança deveriam se reportar ao Programa de Relatórios de Vulnerabilidades do Twitter (TS15)

PP 17 e TS 16 – 2021	1) Possibilidade de transcrição de conteúdo em áudio ou vídeo (PP17) 2) Retirou-se a possibilidade de denúncias de direitos autorais para o serviço do Periscope (TS16)	1) Abriu a possibilidade de uso profissional do Twitter, compartilhando dados de categoria profissional, endereço, e-mail e telefone (PP17) 2) Informação de que dados de interação com postagens seriam públicos (PP17) 3) Possibilidade de configuração de privacidade que impedisse plataformas de vídeo de coletar dados de audiência (PP17)	1) Previsão de comprovação de domínio de conta, no pedido de exclusão de perfil comercial (PP17) 2) Usuários do Brasil, UE e Reino Unido poderiam checar regras de segurança de dados previstas em seus ordenamentos jurídicos (PP17) 3) Diferente da informação divulgada na versão 14 da PP, o Twitter negou a venda de dados de usuários (PP17) 4) Instituiu a possibilidade de cobrança por uso de alguns serviços, mas ainda assim, o usuário teria de concordar com todos os termos de uso da plataforma (TS16) 5) Reino Unido deixa de ser citado como localidade que faria discussões judiciais na Irlanda, subentende-se que a justiça da California serviria também a estes usuários (TS16) 6) Retirou-se a possibilidade de denúncias de direitos autorais para o Periscope (TS16)
PP18 e TS 17 – 2022	Nenhuma referência modificando norma anterior	1) Possibilidade de o usuário levantar questões sobre a PP do Twitter (PP18) 2) Deixou claro que usuários que estivessem utilizando a plataforma com a personificação de outras pessoas estariam violando os termos de uso (TS17)	1) Retirada da figura do Data Protection Office (PP18) 2) Mudança de falsidade ideológica para falsa identidade para quem monta perfil fake (TS17) 3)Proíbe que o usuário tente contornar limitações técnicas da plataforma (TS17) 3) Usuários do Reino Unido são novamente incluídos como base da afiliada do Twitter na Irlanda (TS17)

Fonte: Elaborado pela autora

5.1.3 Documentos avulsos de autorregulação do Twitter

Além das PP e dos TS, foram coletados mais 43 documentos, distribuídos pelo Twitter em sua plataforma, que se referem a regras de comportamento nas postagens

que devem ser seguidas pelos usuários que utilizam a plataforma para compartilhamento de conteúdo gratuito e em programas que exigem pagamento de mensalidade para visualização. As regras gerais para tweetar repelem conteúdo violento, de assédio e práticas semelhantes. De acordo com a plataforma, as normas foram impostas no intuito de manter um ambiente com liberdade e segurança para o diálogo público.

De acordo com Keller (2020a), no princípio as plataformas digitais moderavam conteúdo baseadas principalmente no US Digital Millennium Copyright Act (DMCA) e na Europa pelo e Commerce Directive. A falta de um arcabouço legal de regulação referente à temática deixou nas mãos dos mandatários das plataformas a decisão de como o assunto seria tratado. A preocupação era a retirada de conteúdo sabidamente ilegal, como terrorismo e pedofilia, principalmente. Porém, as regras da comunidade por vezes avançavam sobre conteúdo não tratado pela Lei, como regras morais e sociais. Muitos governos fizeram vista grossa à retirada de discursos não previstos no arcabouço legal, já que tirava do Estados o papel de censor. Entretanto, a discricionariedade na retirada de conteúdo criou reações na rede e somente assim o assunto ganhou espaço entre os legisladores.

Com relação à segurança, o Twitter elenca a proibição de postagens com glorificação da violência e ameaças, terrorismo, extremismo, exploração de menores, abuso, assédio, propagação de ódio, validação de autores de ataques, incentivo ao suicídio, automutilação, violência explícita, conteúdo adulto, produtos e serviços ilegais ou restritos. Com relação à privacidade, a plataforma alerta que é vedado publicar informações pessoais de usuários como endereço e número de telefone. Além disso, é proibida a publicação de nudez não consensual (Twitter, 2022f).

Em suas Regras do Twitter (2022f) a plataforma avisa que a moderação de conteúdo é feita por meio de regras relacionadas à autenticidade das postagens, que restringe o envio de spam; aplicação de técnicas de manipulação da plataforma; manutenção da integridade cívica das nações, evitando principalmente a manipulação de processos eleitorais; personificação de identidades falsas; utilização de mídias sintéticas e manipuladas; além de infrações relacionadas à proteção de direitos autorais e de marcas. É proibido ainda o envio, publicação ou exibição de conteúdo com publicidade de terceiros.

Keller (2020b) afirma que as plataformas empregam normas autorregulatórias que travam a liberdade de expressão, aplicando moderação vasta e excessiva, de

material legal, somente para evitar disputas judiciais ou regulação estatal. O comportamento das plataformas diante de denúncias para remoção de conteúdo é de exclusão sem checagem ou oportunidade de esclarecimento por parte dos autores. Diante desta realidade, em que conteúdo legal é deletado, o debate público segue interditado. Fuchs (2021) destaca que a nova face do capitalismo de plataforma se traduz também em poder político, influenciando na tomada de decisão dos cidadãos. “O capitalismo digital não seria uma nova fase, mas apenas uma dimensão do capitalismo, mediado pela tecnologia” (p. 10).

Para melhor compreensão do que trata cada uma das categorias referente a comportamento vedado em compartilhamento de postagens, cada seção vai tratar de questões específicas do escopo da pesquisa. No ponto 5.1.3.1 são tratadas as normas referentes ao conteúdo considerado violento, em 5.1.3.2 ficam pormenorizadas as regras aludidas a conteúdo inseguro e ilegal e no ponto 5.1.3.3 denota-se diretrizes relacionadas à privacidade do usuário.

5.1.3.1 Normas referentes a conteúdo violento

A violência tem uma gradação e começa pelo comportamento abusivo, entendido pelo Twitter como a tentativa de assédio, intimidação ou silenciamento de voz. De acordo com a política de combate ao comportamento abusivo, são proibidas publicações que envergonhem ou rebaixem indivíduos ou grupos de pessoas. Medidas corretivas incluem o contato com perfis, que na interpretação da plataforma, estejam sofrendo intimidação. Além da busca ativa, são analisadas também denúncias referentes a tweets e conversas privadas via direct (Twitter, 2022g).

Desejar a morte, danos físicos ou sofrimento a alguém é vedado. Assédio sexual também está incluído nesta política e inclui compartilhamento de conteúdo sexual não consensual, objetificação e solicitação de atos sexuais. Esta política condena o uso de insultos, palavrões e calúnia no intuito de intimidar um indivíduo ou grupo de pessoas. E ainda, publicações que neguem a ocorrência de violência em massa, como tiroteio em escolas e ataques terroristas. Vítimas deste tipo de ação são incentivadas a procurar ajuda policial, além de fazer a denúncia propriamente dita à plataforma. De acordo com as regras, o Twitter pode trabalhar em conjunto com as autoridades policiais, fornecendo informações para a identificação do autor ou autores das ameaças (Twitter, 2022g).

Burgess (2021) sinaliza que o antagonismo nas conversas online é parte da cultura do Twitter, construída desde o princípio da história da plataforma. A dificuldade em combater a ação coordenada de ataque a indivíduos ou grupos minoritários é amplificada pela possibilidade de contato imediato dos usuários com as conversas em alta na plataforma, por meio de hashtags que são listadas nos *trending topics*. Por conta da natureza da plataforma, fica difícil combater excessos que ocorrem em discussões em questões de minutos, com aglomeração de *posts* por *hashtag* e marcação de mais usuários para entrada na conversa.

A expressão do comportamento abusivo, de acordo com a plataforma, está diretamente ligada a ações de assédio contra grupos marginalizados que foram historicamente sub-representados. Ações que denotam ódio, preconceito ou intolerância são inaceitáveis. Denúncias de ameaças em *posts* ou via mensagem direta neste sentido são analisadas com prioridade e tem política de tolerância zero, com suspensão imediata das contas. A incitação à violência, genocídio, linchamento e o desejo de que algo ruim aconteça a pessoas por conta de etnia, cor, raça, orientação sexual ou religiosa são comportamentos previstos nesta política (Twitter, 2022h).

O Twitter informa que identifica apelidos, xingamentos, insultos, comentários sexistas, racistas e publicação de símbolos referentes a segregação, além de deturpação de momentos históricos como o Holocausto. Qualquer usuário pode denunciar este tipo de ação na plataforma, independentemente de serem ou não alvos da ação. A punição pode ser feita com rebaixamento do tweet, desqualificação para distribuição, exclusão do post ou recomendação de produto, solicitação para remoção do conteúdo ou suspensão da conta, dependendo da gradação da ofensa emitida (Twitter, 2022h). Flew (2018) concorda que as punições mais brandas para comportamento inadequado nas plataformas digitais devam estar sob a égide de normas autorregulatórias, com sanções mais severas a cargo de normas de Estado. Só assim as sanções seriam efetivamente aplicadas.

O Twitter instrui as vítimas de comportamento abusivo a primeiramente lidar com a situação. Recomendações para deixar de seguir o agressor, bloquear a conta e denunciá-la fazem parte das instruções de endereçamento inicial do problema. Caso haja insistência, a plataforma recomenda a denúncia do perfil e o registro policial da ocorrência. Instrui o usuário a fazer *print* dos *posts* agressivos, para produzir prova da

ação, além de denúncia sobre comportamento reiterado e frequente, inclusive fora da plataforma (Twitter, 2022i).

Mesmo pessoas que não sejam vítimas diretas podem denunciar este tipo de comportamento. A plataforma justifica que não bloqueia o IP de contas denunciadas por risco de impedir erroneamente o acesso de contas que não cometeram abuso. Segundo o Twitter, endereços de IP podem ser facilmente burlados e isso representaria um risco de censura a contas idôneas (Twitter, 2022j). Os usuários são incentivados a auxiliar quem está sendo vítima de assédio por meio de escuta ativa e denúncia. Dependendo da intimidade com a vítima, é recomendado o incentivo à busca por ajuda profissional de terapeuta, advogado, além da política (Twitter, 2022k).

De acordo com o Twitter, esta política reconhece como violência a terceiros o incentivo à automutilação e ao suicídio. Declarações que demonstram intenção de autoflagelo, agressão, oferecimento de recompensa a quem praticar o ato ou matar alguém são removidas mediante denúncia. A plataforma compreende que nem sempre a intenção do autor do tweet é de consumação da violência, mas a postagem pode significar uma figura de linguagem, como quando alguém que posta: “Vou te matar por ter dado spoiler do filme”. Porém, cada caso é analisado em seu contexto individual (Twitter, 2019a).

Belli (2019) alerta, porém, que os conteúdos que geram maior engajamento nas redes sociais são justamente os ofensivos. As mensagens de agressão e assédio, em geral, são seguidas por troca de insultos entre as partes, incitando a reação da audiência, que, em regra, toma parte na desavença. O resultado disso é um aumento no engajamento, que potencializa a coleta de dados pessoais, base econômica das plataformas. Portanto, insultos geram matéria prima de troca mercantil, residindo neste ponto um dilema: como limitar um conteúdo que gera retorno financeiro?

Uma ressalva feita pelas normas ressalta que o Twitter é um ambiente em que pessoas de diferentes visões, ideologias e contextos sociais estão discutindo em um mesmo ciberespaço. Com isso, há controvérsias que são bem-vindas, porém, quando a plataforma detalha que ao se deparar com conteúdo considerado por ela ofensivo, o usuário vai ser convidado a revisar o *post*. A ação pode incluir edição ou retirada do material do ar, mas o aviso está disponível apenas para usuários da plataforma em inglês (Twitter, 2022l).

Para Gorwa (2020) o ocidente democrático ainda não encontrou um ponto de equilíbrio sobre o que de fato deveria ser considerado conteúdo inapropriado no

ciberespaço. Os legisladores alemães vêm pressionando o parlamento europeu que defina como ilegal online aquilo que já é ilegal offline, conferindo, assim, um parâmetro de moderação. O assunto não é unanimidade e muito ainda precisa ser discutido para que os países democráticos mantenham um ciberespaço baseado nos ideais de liberdade de expressão, porém, com responsabilidade.

O Twitter informa que entende a automutilação e o suicídio como problemas sociais. Segundo as regras, a plataforma faz a moderação de conteúdo utilizando gatilhos de linguagem como: “o mais eficiente”, “o mais fácil”, “o melhor”, “o mais bem-sucedido”, “você deve”, “porque você não faz tal coisa”. Distúrbios alimentares como anorexia e bulimia estão incluídos nesta política. Publicar estratégias para a prática de violência contra si mesmo é vedado. Porém, publicações que relatem experiências de superação (sem detalhamento de autoflagelo), grupos de apoio e debates com pesquisas sobre o tema são exceção à regra. Além da moderação do conteúdo, a polícia pode ser chamada para atender casos de emergência (Twitter, 2022m).

Além destas ações, o Twitter divulga serviços de apoio nos Estados Unidos, por meio National Suicide Prevention Lifeline[37] e a International Association for Suicide Prevention.[38] O Twitter disponibiliza o acesso a uma equipe de alerta da plataforma. O link no documento remete a um formulário que o(a) usuário preenche e de acordo com a plataforma é enviado a uma equipe especializada a lidar com este tipo de situação. O documento elenca comportamentos de alerta de usuários propensos à prática de automutilação e suicídio como *posts* depressivos, de desespero, sobre morte como única solução, comentários sobre tentativas de suicídio, identificação de autoflagelo ou tentativa de suicídio ou mudança brusca de humor (Twitter, 2022n).

A plataforma proíbe a veiculação de conteúdo de ataque a um indivíduo ou grupo de pessoas. De acordo com as regras, a glorificação da violência pode incentivar outras pessoas a praticarem os mesmos atos. Classifica-se como eventos violentos casos relacionados a ataques a grupos delimitados por questões étnicas,

---

37 O National Suicide Prevention atende nos Estados Unidos pelo número 988. Foi fundado em 2005, tem 160 pontos de atendimento que funcionam 24 horas, sete dias por semana. Informações disponíveis em: https://988lifeline.org/ Acessado em 18/08/2022

38 A Internacional Association for Suicide Prevention relaciona a rede de serviços ao redor do globo que trabalham com a prevenção a suicídio. Quando o usuário clica no link no site é remetido a uma página onde encontra a entidade em seu país representante da associação. No Brasil é o Centro de Valorização à Vida (CVV), que foi fundado em São Paulo, em 1962. Foi reconhecido como entidade de Utilidade Pública Federal e funciona pelo número 188, em 24 estados e no Distrito Federal. São mais de 400 voluntários que atendem nas linhas que funcionam 24 horas, sete dias por semana. Informações disponíveis em: https://www.cvv.org.br/o-cvv/ Acessado em 18/08/2022.

religiosas, de gênero, orientação sexual, idade, deficiência ou doença grave. As normas vedam apoio, comemoração, elogio ou tolerância a crimes praticados com esta vertente. Comentários como: “Fico feliz que isso tenha acontecido” e “Queria que mais pessoas fizessem o mesmo”, são compreendidos como incentivo à mesma prática (Twitter, 2019b).

Estas regras incluem atos violentos praticados por civis, que resultaram em morte ou lesões sérias, como tiroteios em massa e as ações praticadas por grupos extremistas/terroristas ao redor do globo. Eventos violentos como o Holocausto ou genocídio em Ruanda são alguns exemplos. Porém, são exceção à regra os atos de violência praticados por Estados-nação instituídos. As violações a esta política podem ser denunciadas por qualquer usuário da plataforma por meio do app no celular ou então via computador, utilizando formulários de denúncia. A punição ao infrator desta política vai de pedido de remoção de publicação, suspensão de conta ou banimento. O grau de aplicação da penalidade depende do status do usuário e se o caso é de reincidência (Twitter, 2019b).

As regras estabelecem a remoção de perfis de autores de ataques terroristas, extremistas e de violência em massa, assim como tweets de manifestantes neste mesmo sentido. De acordo com a plataforma, os tweets são monitorados para evitar que a mensagem dos terroristas seja passada à frente. A compreensão é de que mesmo não tendo a intenção de incentivar a violência, a propagação de informações sobre os eventos e dos manifestos pode fomentar novos ataques. Portanto, publicações posteriores a estas ações são moderadas com rigor pela plataforma e a manutenção dos tweets sobre o assunto consideradas individualmente (Twitter, 2022a).

O Twitter classifica como manifesto as declarações de autores de ataques violentos que justificam suas ações, emitem opiniões e motivações. Pode ser emitido por documento escrito, declaração em redes sociais, vídeo, link externo, entre outras possibilidades de formato. Pode conter a ação ou intenção de agir. O autor pode estar relacionado a uma organização terrorista ou declarar-se membro dela. Perfis e publicações destes indivíduos ou cúmplices são derrubados. Mesmo conteúdo de discussão, que é permitido, terá imagens cobertas, com aviso de post sensível. São exceção a esta política as publicações de indivíduos que resistiram ao ataque e demais atos de contra-ataque a ações terroristas ou de violência em massa (Twitter, 2022a).

É considerada como mídia sensível toda a publicação de material excessivamente sangrento, violento ou de conteúdo adulto. Para publicação deste tipo de conteúdo, o usuário precisa classificar a sua conta como de um perfil sensível. As mídias ficarão cobertas e para assistir o usuário vai precisar consentir com a possibilidade de entrar em contato com este tipo de material. Usuários menores de 18 anos ou que não tenham divulgado sua data de nascimento ficam excluídos do compartilhamento de conteúdo adulto. A plataforma classifica as mídias sensíveis em categorias, para melhor exemplificação trazemos o Quadro 8 detalhando os exemplos.

Quadro 8 – Exemplos de mídia sensível publicadas no Twitter

CATEGORIA	**EXEMPLOS DE PUBLICAÇÃO**
Violência explícita	- Crimes ou acidentes - Lutas físicas - Abuso físico de crianças - Fluidos corporais incluindo, sangue, sêmen, fezes etc. - Lesões físicas graves, com ferimentos visíveis - Animais feridos ou mutilados
Conteúdo adulto	- Nudez total ou parcial, incluindo partes desnudas do corpo - Simulação de atos sexuais - Relação sexual ou qualquer outro ato sexual
Conduta sexual violenta	- Estupro ou qualquer outra forma de abuso sexual, que ocorrem sem consentimento da vítima - Violência sexualizada, na qual a pessoa não tenha consentido, que gere ferimentos
Violência gratuita	- Seres humanos mutilados ou desmembrados - Restos humanos carbonizados ou queimados - Órgãos internos ou ossos expostos - Tortura ou matança de animal
Imagens de propagação de ódio	- Logotipos, símbolos ou imagens que tenham conotação de promover hostilidade contra grupos específicos, como a suástica nazista - Reprodução de imagens de indivíduos em condições degradantes ou alteradas para aferir características animalescas - Manipulação para incluir cenas de extermínio em massa, incluir brasões amarelos com a Estrela de Davi, em referência ao Holocausto

Fonte: Elaborado pela autora com base no documento da Política de mídia sensível no Twitter

Caso o usuário entre em contato com uma mídia sensível, o Twitter recomenda que o *post* seja denunciado. A sinalização para a plataforma emite um alerta e os moderadores entram em ação para analisar caso a caso. Segundo a plataforma, o

dono do perfil não é avisado e nem o conteúdo retirado do ar imediatamente, isso ocorreria apenas depois de análise. Para evitar a visualização de mídia sensível, o usuário é instruído a proteger sua conta. A customização de visualização pode ser feita na aba privacidade, com isso, o perfil estaria relativamente protegido da visualização de material sensível ou impróprio (Twitter, 2022o).

De acordo com a plataforma, a promoção de atividade extremista, terrorista, de violência em massa ou prática de atividade ilegal é combatida de acordo com normas nacionais e internacionais. Os critérios do Twitter para definir grupos extremistas são: objetivos declarados, envolvimento em atos de violência e propagação das ações neste sentido e promoção de ataques. Para a designação de organizações é levado em consideração o conjunto de indivíduos unidos com uma finalidade e visando sistematicamente a violência contra civis. A promoção de recrutamento de simpatizantes, adeptos, partidários, fornecedores e distribuídos dos produtos e serviços que incentivam atos relacionados à temática, utilização de insígnias e símbolos do grupo extremistas são vedados (Twitter, 2020e).

A reconsideração com relação a grupos conhecidos pela prática de ações violentas passa pela eleição de membros da organização em pLeitos democráticos. Com relação às publicações, leva-se em consideração a possibilidade da veiculação de conteúdo educativo ou documentários. Não havendo proibição quanto a organizações governamentais. Novamente, a denúncia referente a esta questão pode ser feita por qualquer usuário da plataforma (Twitter, 2020g).

Com relação à exploração sexual de crianças e adolescentes, a política da plataforma repele qualquer material que mostre ou promova este tipo de tema. Isso inclui qualquer tipo de mídia, imagem, texto, ilustração ou arte relacionada. A plataforma detalha a proibição de postagens com representações visuais de menores em atos sexuais ou sugestivos, imagens geradas por computador na mesma situação, comentários sexualizados a menores ou sobre crianças e adolescentes, além de links para sites de terceiros que divulgam material de exploração sexual de crianças e adolescentes. São vedados ainda o compartilhamento de *posts* sobre fantasias com menores ou a participação em atos do gênero, pedido para obter material desta temática, recrutar, anunciar ou expressar interesse em menores para eventos sexuais, enviar mídia sexualmente explícita a menor, tentar iludir ou por meio de chantagem obter imagens sexuais de menores, identificar vítimas de abuso sexual por nome ou

com imagem, promover ou normalizar a atração sexual por menores como forma de identidade ou orientação sexual (Twitter, 2020h).

Em contrapartida estão liberadas as postagens referentes à discussão e combate à exploração sexual de menores, assim como conversas sobre grupos de apoio, que auxiliem as vítimas. Compartilhamento sobre formas de denúncia à exploração sexual também é incentivado. Imagens de nudez de menores em contextos científicos, educacionais, artísticos e relacionados à imprensa são permitidos, porém, monitorados com cuidado. Qualquer pessoa pode denunciar à infração destes casos e em situação afirmativa de abuso a plataforma retira o conteúdo do ar e o perfil é suspenso de forma imediata e permanente. Além disso, links de terceiros são denunciado ao The National Center for Missing & Exploited Children (NCMEC)[39] (Twitter, 2020h).

5.1.3.2 Normas referentes a conteúdo inseguro ou ilegal

A utilização da plataforma para a promoção de produtos ou serviços ilegais é proibida. As normas incluem a compra, venda ou facilitação na transação de produtos e serviços ilegais ou então regulados por Lei. Os *posts* relacionados a esta temática, de acordo com a plataforma, são moderados por pessoas e não algoritmos. Autoridades policiais podem ser chamadas para intervir. Fazem parte desta política posts relacionados: produtos e serviços falsificados; medicamentos e substâncias controladas; tráfego humano; produtos feitos a partir de espécie protegida ou ameaçada de extinção; serviços sexuais; produtos roubados; e armas de fogo, munição, explosivos e instruções para produção de artefatos como bombas e armas impressas em 3D (Twitter, 2019d).

A plataforma alerta para uma prática comum, a utilização de aplicativos que prometem seguidores gratuitos. O Twitter elenca os seguintes riscos na utilização destes apps: a conta pode ser comprometida; a conta pode publicar automaticamente mensagens com URLs de spam, curtir, retweetar e seguir contas aleatórias; obter

[39] NCMEC deu origem à International Center for Missing & Exploited Children que dá suporte a governos, polícia, legisladores, indústria, sociedade civil e serviços de saúde no combate à exploração sexual infantil. A ação é de programas preventivos ao sequestro e exploração sexual, assim como ação em casos de desaparecimento de menores. O braço internacional da ONG nasceu depois do pedido de ajuda do governo Belga, que teve de lidar com um caso de exploração sexual de menores praticado por um cidadão do país contra meninas, em 1996. A ICMEC foi criada em 1999 e tem escritórios representantes na Austrália, Brasil e Singapura. Informações disponíveis em: https://www.icmec.org/about/ Acessado em: 18/08/2022.

seguidores falsos ou comprometidos; ser forçada a autenticar apps adicionais; e incorrer em violações que podem provocar o bloqueio ou suspensão da conta. A utilização destes apps não é recomendada pelo Twitter (Twitter, 2022p).

O Twitter tem uma política de identificação e sinalização de links inseguros. De acordo com a plataforma, eles são identificados por meio de banco de dados que identifica sites de *phishing*, que enganam pessoas para obter dados confidenciais; *malware* (vírus) ou spam; e ainda sites que violam os TS. Parceiros externos também são utilizados para avaliar e colocá-los na lista de inseguros ou impróprios (Twitter, 2022q).

A tentativa de manipular a utilização da plataforma também está prevista nas regras do Twitter. São vedados comportamentos que visem manipular ou prejudicar a experiência do usuário, como o envio de spam, induzindo o usuário a participar de ação em massa agressivas ou enganosas. Em muitos casos, spam é utilizado para direcionar usuário de uma conversa a propagandas para consumo de produtos ou serviços. Tem ainda a ação de dar a ideia enganosa de engajamento a uma página ou publicação de forma artificial (Twitter, 2022b).

Contas falsas e automação também podem dar a impressão de popularidade a perfis ou conversas de forma inorgânica, são exemplos destas iniciativas: contas sobrepostas – que nada mais são do que operação simultânea de contas com perfil e interesses semelhantes; contas que interagem mutuamente – manipulando o algoritmo, dando a ideia artificial de engajamento; coordenação – criar várias contas para publicação de *posts* duplicados, usar *hashtags* semelhantes ou idênticas, dando ideia de *crowd*; coordenar ou recompensar financeiramente contas que se proponham a engajar com publicações e perfis (Twitter, 2022b).

O Twitter veda o inflacionamento artificial das métricas, que pode ser feito por meio de compra e venda de interação com tweets e contas; promoção de apps que prometem a adesão de seguidores gratuitos; coordenar a troca de seguidores mutuamente por meio de pagamento, em ações conhecidas como “trens de seguidores”, “decks” e “Retweet por Retweet”; transferir, vender ou alugar perfis na plataforma. O uso indevido das funções também é prática proibida, entre elas está o uso de mensagens em *tweets* e directs de forma indiscriminada, a prática de publicar o mesmo *post* várias vezes, fazer rotatividade de seguir perfis, interação agressiva com publicações, incluir perfis em listas de menção, usar assunto popular em *hashtag* para conseguir visualizações (Twitter, 2022b).

Interessante observar que depois de elencar as informações relacionadas à violação das regras, as exceções são muito próximas do que é proibido como: publicar links sem comentários, de forma ocasional; coordenar com outras pessoas a divulgação de ideias, ou de uma causa comum, operar várias contas com identidades, finalidades ou casos de uso distintos, com interação mútua, desde que respeitem as normas, seriam exemplos desta prática organizações com comitês separados geograficamente, administração de uma conta pessoal e outras com pseudônimos ligados a *hobbies* ou iniciativas e até *bots* de *hobbies* artísticos. Contas sinalizadas como infratoras das regras podem ter pedido de checagem por *reCAPTCHA*, que é uma proteção contra robôs, ou ainda receber bloqueio, suspensão ou banimento (Twitter, 2022b).

Para manter a conta em segurança o Twitter faz algumas recomendações: senha forte, checagem por duas etapas, solicitação de link ou código para redefinição de senha, atenção ao site de acesso à plataforma, não fornecimento de senha de acesso a terceiros, utilização de antivírus e navegador atualizado. Há um aviso de que o Twitter não liga ou envia mensagens pedindo senha aos usuários. São enviados alertas por acessos via plataformas anteriormente não utilizadas (Twitter, 2022r).

A violação de direitos autorais está tipificada no Brasil como crime. O artigo 184 do Código Penal brasileiro diz que violar direito de autor e conexos podem gerar detenção de 3 meses a um ano, além de multa. Quando a intenção é aferir lucro, a infração pode ter pena entre 2 e 4 anos de prisão, mais multa (Brasil, 1984). Nos Estados Unidos, o uso indevido de material autoral está previsto no DMCA e na União Europeia iniciativas como Safe Harbor, Stop Online Piracy Act e Protect Intellectual Property Act, que foram diretivas em busca de dirimir o problema do uso indevido de material com proteção aos direitos autorais (Silva, 2021).

O Twitter trabalha principalmente as diretivas presentes no DMCA para tratar problemas relacionados à infração aos direitos autorais na plataforma. As normas reconhecem a Lei estadunidense para notificação e retirada de conteúdo contrário à norma. Quando o usuário clica no link para saber se é proprietário de direitos autorais é remetido ao site copyright.gov do governo dos EUA que trata do assunto. Caso o usuário seja alvo de denúncia de violação de direitos autorais deve fazer uma retratação ou contra notificação, caso seja o dono dos direitos do material postado. Todo o processo corre segundo a Lei estadunidense e o processo deve ser feito via

plataforma e rede Lúmen. Há recomendação que o infrator procure ajuda de um advogado e o Twitter informa que não dá assistência jurídica (Twitter, 2022s).

As marcas registradas têm seus nomes, logotipos, frases ou mesmo dispositivos de identidade protegidos. Portanto, usá-los sem autorização é proibido. Neste sentido, a plataforma condena a tentativa de enganar demais usuários sobre representação da marca ou venda de cópias falsificadas. As violações de marcas podem incluir o uso de símbolos em perfis não pertencentes à marca. Neste quesito são verificadas pela plataforma apenas denúncia da própria marca ou do detentor dos direitos dela (Twitter, 2019c).

Mídias manipuladas, com intenção de causar confusão ou ilusão sobre um fato, pessoa ou contexto estão previstas como mais uma vedação do Twitter. A política da plataforma prevê que conteúdo fabricado ou manipulado com intenções enganosas serão considerados como infração grave às regras de utilização do serviço. Quando não há a exclusão, pode, no entanto, haver adição de rótulo, tarja, desativação de distribuição e de curtidas, com fornecimento de um link ao autor para se explicar. A alteração inclui a edição a ponto de distorcer contexto e mensagem original, alteração de compreensão da mídia por modificações feitas, uso excessivo de filtros para simular uma situação inexistente. Há uma preocupação adicional da plataforma quando a mídia fabricada está sendo compartilhada como autêntica, induzindo a erro de autoria, época ou fato. Em última instância, quando a mídia sintética causa confusão na oferta de serviços públicos, ameaça à segurança de grupos ou pessoas e pode causar instabilidade civil (Twitter, 2022t).

A tentativa de manipulação cívica está prevista, principalmente no sentido de interferência em eleições, censo, referendos e votações. Publicações com tentativas de enganar ou distorcer dados podem ter a distribuição impedida. Estas práticas são consideradas antiéticas, mesmo que tenham conotação humorística ou satíricas. Alegações enganosas, que causem confusão no exercício da vontade popular, tentativas de intimidar ou dissuadir a participação são marcadas pela plataforma ou removidas. Polêmicas envolvendo má-fé e informações não checadas sobre fraude em processos eleitorais, personificação de partido ou grupo político também estão vedadas (Twitter, 2021c).

Em 2019, o TSE chegou a fazer um acordo com as redes sociais, entre elas o Twitter, num compromisso de verificação sobre a propagação de notícias fraudulentas, numa tentativa de prevenir ações como as ocorridas nas eleições de

2018. Nas eleições municipais, a rede proibiu o impulsionamento de mensagens de campanhas políticas e autorizou os usuários a denunciar *posts* neste espectro (Amato *et al.*, 2022). De acordo com Barbosa (2022), a democracia depende de um marco regulatório das plataformas principalmente no que tange à questão eleitoral porque processos inteiros podem ser manipulados, por conta do avanço na utilização destas ferramentas digitais em campanhas. União europeia e até mesmo os EUA, reconhecidamente reticentes quanto à regulação, têm tratado do assunto com zelo, para evitar novos casos como da Cambridge Analytica nas eleições de 2016 estadunidenses, caso já citado no capítulo 2 desta tese, quando falamos da segurança e privacidade do usuário nas redes sociais.

Ao mesmo tempo em que tem esta política rígida com relação a estes comportamentos, o Twitter informa que não configura desrespeito a estas regras as declarações imprecisas sobre funcionários do governo eleito ou indicados, partidos políticos e candidatos. Ainda estão livres de sanção conteúdo orgânico polarizado, tendencioso, hiper partidário ou que contenha pontos de vista controversos sobre partidos e políticos. Seguem liberadas discussões sobre resultados de enquetes, votação e participação em games ou outros tipos de entretenimento, uso de pseudônimos e paródias para discutir eleições e política. Em caso de denúncia a gradação da punição vai depender da gravidade do ato, podendo ser retirada de conteúdo a *strike* permanente do perfil (Twitter, 2021c).

Uma preocupação dos legisladores é que as plataformas têm se valido de suas próprias regras para banir conteúdo, considerado legalmente aceito. Nos Estados Unidos, o fato de as plataformas preverem em seus Guias da Comunidade o banimento de certos conteúdos, mesmo legais, impede que o assunto seja questionado judicialmente. Como as plataformas retiram conteúdo por pedido de terceiros, estes podem ter outras intenções quando reportam uma denúncia, como prejudicar competidores, desafetos ou críticos. Uma constatação de vários estudos demonstra que a retirada de conteúdo poucas vezes recebe o pedido de contraprova (Keller, 2020a).

De acordo com o Lúmen (2022), até 2021 foram contabilizados mais de 18 milhões de pedidos de retirada de postagens das plataformas digitais nos EUA. Lúmen é um projeto de pesquisa da Universidade de Harvard, que investiga a moderação de conteúdo na internet desde 2002. Os dados são enviados voluntariamente pelas próprias plataformas e referem-se a denúncias de conteúdo inapropriado ou pedidos

via justiça de material ilegal. O banco de dados do projeto tem crescido a uma velocidade de 40 mil pedidos por semana, na contemporaneidade.

5.1.3.3 Normas referentes a conteúdo relacionado à privacidade do usuário

Esta seção trata das regras referentes à visualização de posts, possibilidade de compartilhamento de conteúdo e marcação do usuário por terceiros. A plataforma alerta que a experiência do usuário pode ser customizada com ferramentas como seguir, silenciar, bloquear, denunciar, proteger, entre outras. É possível impedir a própria visualização de conteúdo sensível, evitar que outras pessoas possam marcá-lo em um *post* e que identifiquem sua localização (Twitter, 2022u).

As informações utilizadas pelo usuário na confecção de um perfil são sempre públicas e incluem a foto, *bio*, localização e endereço de site, quando houver. Porém, é possível ocultar ou restringir a determinados grupos as informações como data de nascimento, por exemplo. Em específico a data de nascimento é utilizada por anunciantes para divulgação de produtos indicados a maiores de 18 anos (Twitter, 2022y)

Por padrão os *tweets* são públicos, mas também é possível restringir a sua visualização. Os *tweets* privados não podem ser retweetados e apenas seguidores do perfil estão aptos a visualizá-los. Perfis com *tweets* protegidos não têm postagens relacionadas nas plataformas de busca e as mídias divulgadas não podem ser compartilhadas (Twitter, 2022x). A plataforma alerta, porém, que a tela do computador pode ser capturada e a informação se tornar pública. Para que toda a audiência da plataforma, e de fora dela, consiga visualizar a mensagem é preciso desproteger os *tweets* (Twitter, 2022w).

A plataforma veda o compartilhamento de informações privadas dos seus usuários, assim como mídias privadas sem autorização de divulgação. Localização física, endereço residencial, número de telefone, e-mail, documentos pessoais, informações financeiras, dados médicos e biométricos, coordenação de eventos para encontrar a pessoa utilizando GPS, compartilhamento de mídia privada, fazem parte desta categoria. Porém, figuras públicas estariam de fora desta política, assim como compartilhamento de informações sobre locais de trabalho, descrições de aparência física, data de nascimento, fofocas, rumores, acusações e alegações, assim como

capturas de telas com mensagens, a menos que contenham informações privadas de terceiros (Twitter, 2022c).

A divulgação de mídia privada de terceiros é outro comportamento vedado na plataforma. Vídeos com imagens íntimas, sem consentimento das pessoas retratadas, é proibida a divulgação. Este tipo de *post* ficou conhecido como *revenge porn,* em tradução livre, vingança pornográfica. O resultado deste tipo de postagem pode envolver prejuízos emocionais, físicos e financeiros para as vítimas. Fazem parte desta categoria vídeos de câmeras escondidas, fotos secretamente tiradas de partes íntimas, imagens manipuladas utilizando o rosto de uma pessoa e corpo de outra, vídeos capturados de telas de computador e até oferecimento de recompensa em troca deste tipo de conteúdo. Pornografia adulta consentida está fora do escopo da regra (Twitter, 2019d).

Embora a plataforma não obrigue o usuário a divulgar seu nome e nem foto no perfil, a identidade falsa é vedada. De acordo com o Twitter, constitui identidade que induz ao erro são aquelas que retratam com semelhança um indivíduo ou marca, tentando se passar por esta outra figura. A utilização de fotos roubadas ou produzidas por computador são formas de camuflar a verdadeira identidade do usuário. Segundo a plataforma, muitas destas contas são utilizadas para a aplicação de golpes, manipulação de atos cívicos, práticas de abuso e assédio (Twitter, 2022y).

As denúncias com relação a este tipo de comportamento são checadas a partir da verificação da conta, com relação à utilização de imagem roubada ou gerada artificialmente e quais os tipos de mensagem que posta e compartilha. Em contrapartida, são comportamentos permitidos contas de mesmo nome sem mais características, contas com uso de pseudônimo, contas de paródias, superfãs e fãs clubes (Twitter, 2022y).

Existe uma política específica para contas de paródias, comentários e fã-clubes. Segundo esta norma, não são permitidos os perfis que são criados com a intenção de iludir, confundir ou induzir ao erro. Portanto, não é permitido personificar a identidade de outra pessoa. São reconhecidas dentro desta categoria contas utilizadas para discutir, satirizar ou compartilhar mensagens sobre o tema do perfil e mesmo fazendo uso de itens de identidade do assunto do qual trata, não iluda usuários no sentido de se fazer passar pelo objeto de discussão. São reconhecidamente contas de notícias ou de interpretação de personagens (Twitter, 2022z).

Para evitar confusão, o Twitter recomenda que a descrição da conta no perfil ou na *bio* se identifique como pertencente a esta categoria utilizando palavras como “fake”, “paródia”, “fã” e “comentário”. Utilizar no nome de usuário ou *bio* designações como “oficial”, no intuito de enganar seguidores, é vedado. Contas denunciadas com referência a esta regra poderão ter a chance de revisão da apresentação e são temporariamente suspensas, até a correção, ou então permanentemente excluídas, dependendo de questões como reincidência (Twitter, 2022z).

Com relação a publicidade, o Twitter permite que empresas anunciantes possam rastrear a idade dos usuários, para impedir que conteúdo impróprio seja visualizado por menores de 18 anos. O rastreamento da idade é feito com referência à data de nascimento informada pelo usuário na confecção de um perfil. Para contas que não informam a data, os conteúdos adultos são bloqueados (Twitter, 2022a2).

Para evitar a prática de roubo de informações como o *phishing*, o Twitter informa que utiliza o aviso de alerta para quem clicar em hiperlinks, ou então o bloqueio para links externos. A política para identificação de links suspeitos passa por fornecedores externos especializados em combate de *malware*, parcerias colaborativas com ONGs especializadas em segurança na internet, tecnologias e ferramentas internas e denúncias. Links bloqueados ao serem clicados emitem a seguinte mensagem: “Não é possível concluir essa ação porque esse link foi identificado pelo Twitter ou por nossos parceiros como potencialmente nociva. Acesse nossa Central de ajuda para saber mais”. O bloqueio pode ser contestado e o caso é analisado individualmente (Twitter, 2020f).

O Twitter informa ao usuário sobre mudança recente de dados do perfil. Assim, em caso de comprometimento da conta é possível tentar recuperar a posse do perfil. Além disso, a plataforma recomenda que o usuário troque a senha de acesso, fazendo a certificação de que o endereço de e-mail segue o mesmo e não corre o risco de ter sido roubado. Aplicativos de terceiros recentemente incorporados devem ser descontinuados e excluídos, porque podem ser a fonte do vazamento de informação e apropriação indevida da conta. Tweets indesejados e spam também devem ser excluídos (Twitter, 2022b2).

5.1.4 Normas para monetização de conteúdo

As normas de monetização de conteúdo no Twitter permitem que usuários ganhem dinheiro com a exploração de produção por seus fãs com ferramentas como Super Follows e Espaços com Ingresso. Os serviços funcionam como assinaturas e ganham destaque com relação aos demais seguidores do perfil. Para fazer parte deste grupo seleto de produtores de conteúdo monetizado o perfil deve cumprir o contrato de usuário por meio dos TS, as regras do Twitter, a Política de Anúncios, devem seguir o Amplify Publisher Faq,[40] e as Políticas de Brand Safety. Uma série de vedações é imposta a quem aderir à monetização de conteúdo (Twitter, 2022c2).

O documento da ferramenta Amplify Publisher Faq relaciona uma série de regras referentes à monetização de conteúdo que pode ser compartilhado em vídeo, cópia de tweet, áudio, imagem, sobreposição de texto e contexto. A relação de conteúdo proibido para monetização inclui conteúdo sexual adulto, direitos autorais e marcas registradas, ódio e extremismo, linguagem profana e ofensiva, produtos e serviços ilegais ou restritos, conteúdo sensível, malicioso e enganoso, spam, violência, censurável ou gráfico (Twitter, 2022c2). Para detalhar o que cada categoria engloba, o Twitter publicou o documento Brand Safety Policy, as normas estão ilustradas no Quadro 9.

Quadro 9 – Conteúdo proibido para monetização no Twitter

CATEGORIA	TIPOS DE PUBLICAÇÃO
Conteúdo sexual adulto	- Representação ou descrição de atos sexuais - Brinquedos sexuais - Órgãos sexuais - Fluídos corporais sexuais - Conteúdo sexual sugestivo - Serviço de acompanhante - Prostituição - Sites de namoro focados em sexo, nudez parcial ou total - Sites de serviço adulto, erotismo e pornografia - Roupas e acessórios sexualmente explícitos - Serviços de aprimoramento sexual
Direitos autorais e marcas registradas	- Distribuição não autorizada de conteúdo protegido por direitos autorais - Serviços que ensinam como burlar proteção contra cópias - Conteúdo enganoso sobre afiliação de marca - Promoção ou venda de produto falsificado
Conteúdo de ódio ou extremista	- Conteúdo inflamável ou incendiário

40 Amplify Publisher Faq é a ferramenta utilizada para monetizar conteúdo no Twitter.

	- Assédio, humilhação, insulto contra raça, credo, cor, gênero, identidade de gênero, idade, deficiência, condição médica, estado de veterano, estado de refugiado ou imigrante - Linguagem com intenção de rebaixar, degradar, ameaçar ou intimidar indivíduo ou grupo - Promoção de glorificação ou afiliação a grupos, associações, organizações criminosas ou terroristas
Linguagem profana e ofensiva	- Qualquer uso de insulto sem censura - Profanação censurada excessiva
Produtos e serviços ilegais ou restritos	- Drogas recreativas ou produtos utilizados para o consumo de drogas - Tabaco e produtos relacionados - Álcool - Jogos de azar, loterias e rifas - Armas e munição - Promoção ou venda de produtos de espécies ameaçadas
Conteúdo sensível	- Desastres naturais - Menções de mortes - Revoltas políticas - Eventos terroristas ou com vítimas em massa - Armas e munições - Promoção ou glorificação de automutilação ou distúrbios alimentares
Spam	- Conteúdo enganoso e malicioso
Conteúdo violento, questionável ou censurável	- Fantasia e violência ficcional - Comportamento desagradável, grosseiro, incluindo intoxicação visível - Imagens educacionais e científicas - Videogames violentos (recomendação de retirada de efeitos de sangue nos jogos) - Animais, incluindo conteúdo que discute danos aos animais

Fonte: Elaborado pela autora com base no documento Brand Safety Policy

De acordo com a plataforma, o rol apresentado é apenas exemplificativo, ou seja, publicações que o Twitter faça relação com referência a uma das categorias acima citadas podem ser incluídas na política de proibição de monetização. As regras para quem descumprir as normas incluem strike da publicação com três graus de punição: advertência, suspensão de utilização da ferramenta de monetização por uma semana e nos casos considerados mais graves por até seis meses (Twitter, 2022d2).

Keller (2020c) sinaliza, porém, que mesmo conteúdo previsto como aceitável dentro das PP ou TS das plataformas pode ser desmonetizado. Pesquisas

demonstram que a moderação do conteúdo muitas vezes é feita por mão de obra terceirizada, que tem indistinta discricionariedade para retirar do ar qualquer material, ficando o usuário à disposição da voluntariedade de quem estiver designado para analisar o seu caso específico. Isso quando o conteúdo foi retirado por algoritmo, recebeu um recurso do usuário e só então terá sua requisição analisada por uma pessoa.

Quanto à idade de utilização, a ferramenta exige idade mínima de 18 anos, verificação de conta, boa recomendação do perfil, ser um produtor de conteúdo ativo, concordância com os TS e o Safe for Ads. Segundo o Twitter, o pagamento pelo conteúdo é feito por depósito ou Paypal, a apuração dos ganhos é aferida por dados analíticos e o montante pago a cada 60 dias, desde que o produtor de conteúdo tenha indicado a monetização no *upload* da postagem e os ganhos tenham atingido ao menos US$ 100 (Twitter, 2022d2).

Para produzir conteúdo e ser monetizado pelo Super Follows além de atender às regras do Brand Safety Policy e Amplify Publisher Faq o usuário ainda precisa somar número igual ou superior a 10 mil seguidores, ter conta ativa a no mínimo três meses e ter publicado ao menos 25 *tweets* nos últimos 30 dias. O Twitter informa, porém, que o Super Follow é um programa aberto apenas a criadores de conteúdo residentes nos EUA (Twitter, 2022e2).

As regras para a produção de conteúdo nesta modalidade são extensas. O usuário concorda com todas elas e assina um compromisso no qual admite não ser funcionário do Twitter, mas sim parceiro. Os usuários que seguirem o perfil adepto do Super Follows pagam uma mensalidade pelo conteúdo. A plataforma repassa parte dos valores para o criador, que deve se comprometer a pagar os impostos pela renda. O juízo da Califórnia foi eleito para a disputa de desacordos comerciais em relação ao serviço (Twitter, 2022f2).

A monetização dos Espaços com Ingressos atende a todo o tipo de conteúdo. Para estar habilitado para o serviço, novamente é preciso atender às normas do Brand Safety Policy e Amplify Publisher Faq, é indisponível para contas afiliadas ao Estado, o perfil precisa ter ao menos mil seguidores e ter apresentado ao menos três espaços no prazo de 30 dias. Esta também é uma ferramenta exclusiva para perfis sediados nos EUA (Twitter, 2022g2).

Quando aceita os termos para criação de conteúdo para os Espaços com Ingressos, o produtor concorda inclusive com a interferência do Twitter na aferição de

preço do *ticket* de entrada para o evento e no monitoramento referente ao material compartilhado. O repasse de valores ao criador de conteúdo atende à discricionariedade da plataforma e revisões sobre repasses não serão feitas para valores inferiores a US$ 50. Os pagamentos são feitos em prazos de 60 dias e novamente a corte da California é mencionada como foro para resolução de disputas. O usuário concorda com a informação de que não é empregado do Twitter, mas parceiro (Twitter, 2022g2).

Com relação à pandemia de Covid-19, reconhecida pela OMS a partir de março de 2020, a plataforma informou, em 2022, por meio do documento Amplify Publisher Faq, que publicações a respeito do assunto que tratassem de taxas de morte, número de infectados e outros tópicos sensíveis continuariam proibidas para monetização. Foi mantida também a vedação de monetização de conteúdo associado a vídeos sobre o tema. Porém, publicações relacionadas à abertura de regiões, retorno de práticas esportivas e retomada de atividade de empresas poderiam ser monetizadas. A primeira política relacionada à monetização de conteúdo relacionado à pandemia foi publicada em 20 de março de 2020, de acordo com a plataforma (Twitter, 2022c2).

5.2 Síntese de resultados sobre normas autorregulatórias do Twitter

Como já mencionado, observamos nas normas de autorregulação do Twitter as informações referentes à liberdade de expressão, privacidade e segurança do usuário. Foram analisados os documentos referentes à Política de Privacidade e os Termos de Serviço desde a criação da plataforma até 2022, somamos a estes documentos as regras específicas sobre postagem de conteúdo.

Em resumo, para a utilização da plataforma as regras impunham idade mínima de 13 anos, a não condução de negócios ilícitos na plataforma, atividade *hacker* e criação de perfil falso. Porém, ao longo da atualização dos documentos, a plataforma admitiu a criação de perfis com pseudônimo e várias contas por um mesmo usuário para expressão de pontos de vista diferentes sobre determinados assuntos. Benedek e Ketteman (2020) alertaram para o risco de o anonimato em perfis acabar protegendo quem propaga conteúdo ilegal. Em 2022, a plataforma sinalizou como infração a personificação de outras pessoas, Leia-se perfis falsos.

O Twitter deixou claro aos usuários que o seu interesse eram os dados de cada um. Quem lesse atentamente os documentos entenderia que a moeda de troca pelo

serviço da plataforma seriam os dados pessoais. Belli (2019) apontou a armadilha das plataformas que dizem oferecer serviço gratuito. O Twitter reconheceu que todas as informações do usuário, inclusive o IP de máquina, poderiam ser compartilhadas com parceiros comerciais, investigações policiais e governos. Por inferência foi possível perceber que o Twitter se autointitula proprietário dos dados, com possibilidade de ceder as informações a terceiros, em caso de venda da plataforma. Autores como Van Dijck (2022), destacaram que uma das maiores afrontas às nações democráticas era a possibilidade de dados pessoais dos cidadãos estarem sob a tutela de empresas particulares, ou mesmo governos.

Conforme a tecnologia evoluiu, as normas autorregulatórias foram sendo modificadas para abarcar as novas ferramentas de acesso à plataforma como o monitoramento de dados de georreferenciamento por uso de *smartphones* ou sinal de *wi-fi*. Mesmo quando o usuário escolhesse excluir sua conta, teria de esperar 30 dias, porém, seus dados permaneceriam sob a tutela do Twitter por 18 meses. Em 2013, a Comissão Europeia criou o Safe Harbor e impediu que dados dos seus cidadãos fossem tratados fora do território europeu. A plataforma estabeleceu Dublin, na Irlanda, como local de tratamento, já para usuários estadunidenses São Francisco, na Califórnia.

Dados bancários dos usuários também figuraram nos documentos do Twitter a partir de 2014. A plataforma previu a retenção de informações de segurança de cartões de crédito em transações comerciais feitas em seu ambiente digital. Além disso, admitiu que dados de compras geravam algoritmos que poderiam ser compartilhados com parceiros comerciais para direcionamento de ofertas de produtos ou serviços, inclusive utilizando os endereços de e-mail dos usuários. Somente em 2020, o Twitter incluiu a previsão de que informações de pagamento passassem a ter a necessidade de anuência do usuário para conclusão de transações.

Em 2016, o Twitter admitiu que o direcionamento de conteúdo poderia ser feito inclusive com base em monitoramento de atividade do usuário fora da plataforma. A partir de 2017, a plataforma começou a dar ao usuário a opção de customizar o direcionamento de conteúdo e escolha de quais dados seriam coletados. Porém, deixou claro que qualquer pessoa que entrasse na plataforma, mesmo como visitante, teria as informações coletadas, armazenadas, tratadas, e, até comercializadas. Deu ao usuário, porém, a possibilidade de pedir a portabilidade dos dados e até mesmo

download das informações coletadas, a partir do RGPD, em 2018. Em 2021 voltou atrás e negou a comercialização dos dados de seus usuários.

Como o Twitter vive da entrada de novos usuários, desde o princípio previu a edição de conteúdo – imagens, textos, vídeos e áudios – dos assinantes para atração de audiência. Segundo o regramento da plataforma, esta edição poderia ser feita inclusive por empresas parceiras do Twitter. Porém, a responsabilização pelo conteúdo em ações judiciais continuava sob a guarda do usuário, mesmo nos casos de posts editados pela plataforma com o objetivo de aumentar o alcance da publicação. Pinheiro e Pinheiro (2021) sinalizaram que este era um comportamento de *gatekeeper* da informação, com Twitter admitindo a curadoria do conteúdo, passando de intermediário a editor do conteúdo.

Mesmo utilizando o conteúdo do usuário para alcance de maior audiência, o Twitter deixou especificado que não pagaria *royalties* aos produtores. Apenas em 2022 passou a estabelecer regras para monetização de conteúdo. Porém, restringiu o conteúdo a ser monetizado e proibiu vários temas (vide Quadro 09, pág. 152). Estabeleceu ainda que o conteúdo da plataforma poderia ser propagado por ela e terceiros em outros meios, como impresso, rádio e televisão. Em 2012, O Twitter estabeleceu um valor de US$ 100 ou o que o usuário pagava pelo serviço, 0, em caso de questionamentos judiciais sobre danos morais, praticados no ambiente digital da plataforma. Estabeleceu São Francisco como estado legítimo para questionamentos judiciais. Em 2016, retirou esta possibilidade de questionamento jurídico, para novamente introduzir a norma em 2020.

A remoção de conteúdo, desde 2009, estava prevista com relação a direitos autorais, utilizando como referência o Digital Millennium Copyright Act (DMCA). Já a remoção com relação a discurso previa a discricionaridade da plataforma em sua compreensão do que seria material ilegal e, ou, imoral. Gillespie (2022) demonstrou que havia uma ação negativa da plataforma, a moderação, e uma positiva, a recomendação, tornando o Twitter o regulador do discurso público. Myers West (2018) conduziu um estudo que demonstrou que os usuários não sabiam por que tiveram posts excluídos e creditaram a ação a denúncias de inimigos pessoais, numa ação humana de desafeto que se transportava do mundo secular para a rede social online.

Em 2016, a criação da Comission´s Code of Conduct for Countering Illegal Hate Speech, na Europa, fez o Twitter prever em suas regras a possibilidade de retirada de conteúdo xenófobo, racista e violento, caso fosse notificado. Poleto e De Moraes

(2019) apontaram que mesmo o Twitter sendo obrigado a excluir conteúdo violento, em 24 horas, nem sempre isso foi feito por conta da previsão de discricionariedade da plataforma. Ao longo dos documentos foi possível observar que o Twitter admitiu a moderação, usando termos vagos – como conteúdo aceitável, bom senso do usuário, discurso de ódio – para decidir o que poderia ou não ser publicado na plataforma. Porém, Gillespie (2018) sinalizou que documentos vazados em 2012, demonstravam como a plataforma moderava conteúdo por atacado, sem parâmetros de legalidade para a exclusão. A partir da moderação em massa de conteúdo, Keller (2020) verificou a falta de limites na discricionariedade do Twitter. Silva *et al.* (2019) pontuaram a inabilidade da plataforma em lidar com conteúdo abusivo e ação de robôs.

A partir de 2020, a plataforma disponibilizou uma lista de assuntos que não seriam aceitos na plataforma como: glorificação da violência e ameaças, terrorismo, extremismo, exploração de menores, abuso, assédio, propagação de ódio, validação de autores de ataques, incentivo ao suicídio, automutilação, violência explícita, conteúdo adulto, produtos e serviços ilegais ou restritos. Alnajahi (2021) pontuou que mesmo melhorando as informações não havia uma especificação do que seria a glorificação da violência ou discurso de ódio, estes parâmetros seriam necessários para que o usuário compreendesse claramente os limites. Burgess (2021) ressaltou que os discursos acalorados sempre geraram maior engajamento na rede social, foram, de certa forma, incentivados ao longo do tempo e fazem parte da cultura do Twitter.

As normas foram sendo especificadas pelo Twitter, com uso de exemplos para determinar o que seria, por exemplo, conteúdo sensível de compartilhamento (vide Quadro 09, pág. 152). Mesmo em caso de conteúdo permitido, alguns, como aqueles envolvendo imagens de violência, só poderiam ser visualizados com prévia anuência do usuário. Houve por parte da plataforma também uma diferenciação entre conteúdo de extermínio, em ataques terroristas e de guerra entre Estados-nações instituídos. Para determinar parâmetros de ação de regulação das plataformas digitais, Gorwa (2020) sugere que se observe o que seria comportamento ilegal, já de acordo com Leis vigentes, que fosse reconhecido como crime no ciberespaço.

No que se refere à proteção de menores, a plataforma tomou precaução com conteúdo de cunho sexual. Foram proibidas divulgações de imagens contendo menores em qualquer situação relacionada à temática. Além disso, imagens sexualizadas de adultos, que forem postadas sem consentimento também podem ser

retiradas. Canais de denúncias foram abertos para que a comunidade pudesse participar com notificações via mensagem ou *flag*. A plataforma também abriu espaço para a discussão do assunto, com temas voltados à conscientização e denúncias de abuso via The National Center for Missing & Exploited Children.

Condução de negociações de produtos e serviços ilegais também figuraram entre as normas de autorregulação do Twitter, como matéria proibida, com previsão inclusive de repasse de informações à polícia para investigação. Identificação de links externos com *phishing* e *malware* para roubo de informações do usuário foram previstos e são mecanismos que podem ser utilizados pela plataforma e membros da comunidade para denúncia.

5.3 Análise de mecanismos legais de regulação no Brasil, EUA e União Europeia

Nesta tese, as normas de regulação previstas na Lei de 2006 a 2022 no Brasil, Estados Unidos e União Europeia foram selecionadas. O início da pesquisa utilizou a data de criação do Twitter, o ano de 2006. A plataforma de compartilhamento de conteúdo que se analisa conjuntamente com o arcabouço legal que compõem os instrumentos de regulação das plataformas de mídia social nos países e bloco econômico em perspectiva. A pesquisa sobre as legislações em discussão ou já aprovadas foi feita a partir das casas legislativas do Brasil e EUA, assim como no Parlamento Europeu.

Os comandos de busca utilizados nas casas legislativas dos países e bloco econômico em perspectiva incluíam as palavras-chaves: plataformas digitais, redes sociais e mídias sociais. Sinaliza-se que foram selecionados apenas os instrumentos regulatórios que tratavam de liberdade de expressão, privacidade e segurança do usuário, que são os parâmetros que esta tese investiga. Dentro do escopo desta pesquisa foram selecionados para análise quatro Leis, uma emenda constitucional e 27 projetos de Lei brasileiros; quatro Leis estadunidenses e mais 95 projetos de Lei dos EUA; e, quanto à União Europeia foram selecionados 12 instrumentos legais.

A análise tem início pelos instrumentos legais brasileiros, na sequência os estadunidenses e por último os referentes à União Europeia. O procedimento de análise inclui a descrição das normas legais, com a inclusão de observações dos estudiosos que já fizeram a interpretação dos documentos via artigos e livros, são

incorporadas ainda informações das entrevistas de pesquisadores e legisladores disponíveis no YouTube, que apresentam o contexto social em que as normas foram confeccionadas. A opção para utilização do último instrumento de análise são as falas de estudiosos e legisladores sobre instrumentos aprovados e para os projetos de Lei que tiveram maior repercussão na mídia no período em que estiveram em discussão.

5.3.1 Mecanismos legais do Brasil

O debate sobre a regulação de plataformas digitais no Brasil, dentro do escopo desta tese, ganhou destaque na agenda legislativa a partir da aprovação do Marco Civil da Internet (Lei 12.965, 2014). Depois deste marco, diversos temas passaram a fazer parte da pauta regulatória das plataformas digitais no Congresso Nacional. Como já evidenciado anteriormente, esta tese foca na análise de projetos de Lei referentes à liberdade de expressão, privacidade e segurança do usuário. Um dos temas mais presentes, dentre as três frentes deste estudo é o da moderação de conteúdo, que trata principalmente da liberdade de expressão.

A apresentação dos projetos legislativos está detalhada no Quadro 10. Os projetos são identificados pelo número, casa legislativa onde foi apresentado, nome do autor, data de apresentação e resumo da proposta legislativa.

Quadro 10 – Projetos de Leis de regulação propostos no Brasil de 2006 a 2022

MECANISMO LEGAL	AUTORES	DATA	RESUMO DA PROPOSTA
Projeto de Lei da câmara nº 7131/2010	Gerson Peres (PP – PA)	14/04/2010	Dispõe sobre a responsabilidade dos proprietários e autores de blogues e mecanismos similares.
Projeto de Lei da câmara nº 1468/2011	Ângelo Agnolin (PDT – TO)	31/05/2011	Cria obrigatoriedade de veiculação de mensagem educativa entre as cláusulas dos termos de aceitação do cadastro de novos usuários de plataformas digitais que permita a publicação sobre os crimes de discriminação.
Projeto de Lei da câmara nº 4565/2012	Professor Victório Galli (PMDB – MT)	17/10/2012	Estabelecia condições adicionais à contratação de provedores de aplicações na internet.
Projeto de Lei da câmara nº 5596/2013	Major Fábio (DEM – PB)	16/05/2013	Proíbe o uso de aplicativos e redes sociais na internet para alertar motoristas sobre a ocorrência de blitz de trânsito.
Projeto de Lei da câmara nº 2498/2015	Aureo Ribeiro (SD – RJ)	11/08/2015	Altera o MCI (LEI Nº 12.965, 2014) (2014), para obrigar as plataformas

			digitais a criarem centros de atenção aos usuários compulsivos de serviços de internet e de redes sociais.
Projeto de Lei do senado n° 347/2016	Vanessa Grazziotin (PcdoB – AM)	19/09/2016	Propunha a alteração do Marco Civil da Internet (Lei 12.965, 2014), para prever consentimento de usuário para receber convite para aderir a redes sociais.
Projeto de Lei da câmara nº 7460/2017	Leandre Dal Ponte (PV – PR)	24/04/2017	Altera o MCI (LEI Nº 12.965, 2014) (2014) e obriga plataformas digitais a retirarem conteúdos que promovam automutilação, exposição à situação de risco de vida ou tentativa de suicídio.
Projeto de Lei da câmara nº 7917/2017	Vítor Valim (PMDB – CE)	20/06/2017	Modifica o MCI (LEI Nº 12.965, 2014) (2014), dispondo sobre a publicação de mensagens de ajuda para o combate ao suicídio em aplicações de busca na internet.
Projeto de Lei da câmara nº 10919/2018	Célio Silveira (PSDB – GO)	30/10/2018	Obriga a identificação publicitária na exibição e na divulgação patrocinadas de produtos e serviços.
Projeto de Lei da câmara nº 2184 e 2185/2019	Roberto Alves (PRB – SP)	09/04/2019	Obriga as plataformas digitais a veicularem campanhas informativas para evitar a distribuição de imagens com nudez de menores.
Projeto de Lei da câmara nº 2463/2019	Coronel Tadeu (PSL – SP)	23/04/2019	Dispõe sobre a limitação de divulgação de imagens e informações em veículos de mídia e redes sociais em situações de ataque massivo a pessoas.
Projeto de Lei da câmara nº 3496/2019	Rejane Dias (PT – PI)	12/06/2019	Dispõe sobre a retirada de conteúdos nas redes sociais que induzam, instiguem ou auxiliem a automutilação.
Projeto de Lei do senado nº 2630/2020 - Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet	Alessandro Vieira (CIDADANIA – SE)	13/05/2020	Estabelece normas, diretrizes e mecanismos de transparência para provedores de redes sociais e de serviços de mensagem privada a fim de garantir segurança e ampla liberdade de expressão, comunicação e manifestação do pensamento.
Projeto de Lei da câmara nº 3993/2020	Dagoberto Nogueira (PDT – MS)	29/07/2020	Dispõe sobre a obrigatoriedade de apresentação de documentos comprobatórios da idade para acesso às plataformas digitais.
Projeto de Lei da câmara nº 4120/2020	Bosco Costa (PL – SE)	07/08/2020	Trata do uso de algoritmos pelas plataformas digitais na internet, assegurando transparência para

			evitar influência na tomada de decisão dos usuários.
Projeto de Lei da câmara nº 4801/2020	Alexandre Frota (PSDB – SP)	02/10/2020	Determina que as redes sociais insiram em suas plataformas alertas sobre o trabalho infantil e suas consequências.
Projeto de Lei da câmara nº 5347/2020	Roberto de Lucena (PODE – SP)	03/12/2020	Cria a Lei de Enfrentamento à Desinformação nas Eleições e estabelece que as plataformas digitais abram espaço para conteúdo da Justiça Eleitoral.
Projeto de Lei da câmara nº 5567/2020	Rubens Otoni (PT – GO)	17/12/2020	Estabelece obrigatoriedade para que as plataformas de mídias sociais para que instituam e mantenham mecanismos de controle de conteúdo.
Projeto de Lei da câmara nº 2762/2021	Airton Faleiro (PT – PA)	10/08/2021	Estabelece a obrigatoriedade de aviso de saúde que especifica em fotos de modelos que forem manipuladas digitalmente com uma *tag*.
Projeto de Lei da câmara nº 2831/2021	Capitão Alberto Neto (REPUBLIC – AM)	16/08/2021	Proíbe a exclusão de postagens em redes sociais sem que se tenha concedido direito de ampla defesa e ao contraditório.
Projeto de Lei da câmara nº 3700/2021	José Guimarães (PT – CE)	21/10/2021	Altera o MCI (LEI Nº 12.965, 2014) (2014), para criar obrigações às plataformas digitais na moderação de discursos de ódio.
Projeto de Lei da câmara nº 188/2022	Marco Feliciano (PL – SP)	09/02/2022	Cria órgão no Ministério das Comunicações para fiscalizar veracidade nas mídias sociais.
Projeto de Lei da câmara nº 397/2022	Marcelo Ramos (PL – AM)	24/02/2022	Estabelece a obrigatoriedade de que PJ, ainda que sediada no exterior, que atuem no País, com prestação de serviços digitais e alcance igual ou superior a 5 milhões de usuários, disponham de representante legal no País.
Projeto de Lei da câmara nº 630/2022	Luciano Bivar (UNIÃO – PE)	18/03/2022	Dispõe sobre a necessidade de os provedores de redes sociais e de serviços de mensageria terem sede e representante legal radicado no país.
Projeto de Lei da câmara nº 2557/2022	Tiago Andrino (PSB – TO) Felipe Carreras (PSB – PE)	04/10/2022	Institui a Política Nacional de Proteção Digital das Crianças e Adolescentes – PNPD.
Projeto de Lei da câmara nº 2768/2022	João Maia (PL – RN)	10//11/2022	Dispõe sobre a organização, o funcionamento e a operação das

			plataformas digitais que oferecem serviços ao público brasileiro.
Projeto de Lei da câmara nº 3046/2022	Sóstenes Cavalcante (PL – RJ)	20/12/2022	Altera o MCI (LEI Nº 12.965, 2014) (2014) para disciplinar bloqueio de conta de parlamentar em redes sociais.

Fonte: Elaborado pela autora

Além dos projetos de Lei que foram discutidos no período de levantamento, entre 2006 e 2022, esta tese analisa ainda quatro Leis e uma emenda constitucional que foram aprovadas no mesmo período que estão descritas no Quadro 11.

Quadro 11 – Leis que regulam plataformas digitais e entraram em vigor no Brasil entre 2006 e 2022

MECANISMO LEGAL	AUTORES	DATA	RESUMO DA PROPOSTA
Lei 12.737/2012 – Lei Carolina Dieckmann	Paulo Teixeira (PT – SP)	30/11/2012	Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.
Lei 12.965/2014 – Marco Civil da Internet	Poder Executivo	23/04/2014	Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.
Lei 13.488/2017 – Altera a Lei 9.504/1997 (Minirreforma da Lei Eleitoral)	Comissão Especial Para Análise, Estudo e Formulação de Proposições Relacionadas À Reforma Política	06/10/2017	Altera as Leis n º 9.504, de 30 de setembro de 1997 (Lei das Eleições), 9.096, de 19 de setembro de 1995, e 4.737, de 15 de julho de 1965 (Código Eleitoral), e revoga dispositivos da Lei nº 13.165, de 29 de setembro de 2015 (Minirreforma Eleitoral de 2015), com o fim de promover reforma no ordenamento político-eleitoral.
Lei 13.7096/2018 – Lei Geral de Proteção de Dados – LGPD	Câmara dos Deputados	14/08/2018	Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.
Emenda Constitucional 115 – Acrescenta o inciso LXXIX ao Art. 5º/CF	Poder Legislativo	10/02/2022	Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais.

Fonte: Elaborado pela autora

A dinâmica de análise vai ter início pela explanação na integralidade dos instrumentos regulatórios já aprovados e em vigor, no caso as Leis e a EC. Posteriormente, os projetos de Leis serão agrupados pelos temas: liberdade de expressão, privacidade e segurança do usuário. Como alguns instrumentos congregam mais de um aspecto, também foram feitos agrupamentos das temáticas propostas para a análise.

Para esta tese considera-se como normas referentes à liberdade de expressão aquelas ligadas à moderação de conteúdo; as normas referentes à privacidade estão relacionadas a tratamento de dados; e, as normas que tratam de segurança se referem ao combate a crimes e situações que oferecem risco à saúde. É necessário fazer uma ressalva, as 73 propostas legislativas apensadas ao PL 2630/2020 estão sumariamente descritas na seção em que o projeto de Lei é analisado. O início da próxima seção se dá com a análise dos instrumentos legais em vigor.

5.3.1.1 Lei Carolina Dieckmann (Lei nº 12.737, 2012)

Uma das primeiras Leis regulatórias, com foco na internet, nasceu após um caso de invasão de privacidade, que foi o vazamento de fotos íntimas da atriz Carolina Dieckmann. Em 2011, a atriz teve o computador invadido e 36 fotos com cenas de nudez foram roubadas e acabaram na rede mundial de computadores, após uma tentativa frustrada de extorsão[41].

A Lei 12.737/2012, que ganhou o nome da atriz, estabeleceu como crime a invasão de dispositivo informático, roubo de informações ou conteúdo, criação de programas utilizados para fazer este tipo de invasão. Há ainda uma previsão de punição para quem divulga ou distribui material obtido desta forma, invadindo equipamento alheio. A Lei prevê pena de seis meses a dois anos para os infratores e ainda pagamento de multa. O texto é curto, são apenas quatro artigos em duas

[41] Dez anos de vigência da Lei Carolina Dieckmann: a primeira a punir crimes cibernéticos (2022). Disponível em: https://www12.senado.leg.br/radio/1/noticia/2023/03/29/dez-anos-de-vigencia-da-lei-carolina-dieckmann-a-primeira-a-punir-crimes-ciberneticos Acessado em 29/05/2023.

páginas que versam principalmente sobre a questão da invasão de privacidade e divulgação de material sem o consentimento do titular.

Almeida *et al.* (2022) observam que a Lei 12.737/2012 foi criada num ambiente em que os legisladores foram pressionados a trabalhar para criar mecanismos de proteção, ou ao menos, punição para invasão de privacidade no ciberespaço. Faltava no arcabouço brasileiro mecanismos legais para julgamento de casos de crimes digitais. Brega (2023) nota que em litígios envolvendo as plataformas no Brasil, o judiciário se valia do Código Civil, de 2002, e do Código de Defesa do Consumidor, de 1990, para julgar situações de material propagado ou transações comerciais na internet, porém, o judiciário só foi legitimamente designado pelos legisladores como solucionador de litígios envolvendo as plataformas digitais a partir do Marco Civil da Internet (Lei 12.965, 2014).

5.3.1.2 Marco Civil da Internet (Lei nº 12.965, 2014)

Apesar da Lei ter sido aprovada em 2014, as discussões para a criação de um mecanismo legal sobre os direitos no ciberespaço começaram a ser feitas em 2007. Dos Santos (2020) destaca que o MCI (Lei nº 12.965, 2014) seria uma resposta à Lei Azevedo (Lei 84/99), que no final dos anos 90 propunha a punição de atividade *hacker* e *cracker*[42] na internet. A Lei inovava e trazia uma redação mais detalhada, que estabeleceu os princípios de uso, direitos e deveres, de usuários e serviços, assim como limites à ação dos entes públicos na internet. A liberdade de expressão é citada logo no 2º artigo do mecanismo legal: “A disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão” (Brasil, 2014).

O MCI (Lei nº 12.965, 2014) trouxe a base de normas para provedores de conexão à Internet e provedores de aplicações de Internet. Foi feita uma diferenciação entre os provedores de conexão, que correspondem à infraestrutura necessária à conexão e os provedores de aplicação que compreendem os serviços prestados via internet, que incluem as plataformas de mídias sociais (Dos Santos, 2020). Os legisladores reconheceram que a internet funciona em escala global, bem por isso, deve primar pela pluralidade de ideias, respeito aos direitos humanos, diversidade, colaboração, livre iniciativa e livre concorrência, respeito ao consumidor, assim como, exercer seu papel de desenvolvimento da sociedade (Brasil, 2014).

---

42 O cracker utiliza suas habilidades tecnológicas única e exclusivamente para a prática de crimes.

A liberdade de expressão, comunicação e manifestação do pensamento são garantias que fazem parte dos princípios do uso da internet, segundo o MCI (Lei nº 12.965, 2014). Dos Santos (2020) destaca que até 2018, 152 pedidos de retirada de conteúdo foram feitos na justiça e apenas 33,5% foram reconhecidos em segunda instância, os outros mais de 60% foram considerados “ilegítimos, infundados ou abusivos” (p. 09). Konopacki e Getschko (2016) reiteraram que um dos maiores avanços do MCI (Lei nº 12.965, 2014) foi a regulação sobre a retirada de conteúdo do ar, que previu a medida por via judicial. A discricionariedade das plataformas para esta supressão de conteúdo poderia ocasionar censura prévia, o que representaria um risco à liberdade de expressão e consequentemente para a democracia.

A Lei reconhece a importância do uso da internet para a formação e participação social do cidadão e prevê a inviolabilidade da vida privada, com reparação por danos morais e materiais em caso de invasão (Brasil, 2014). Amato *et al.* (2021) destacam que inicialmente a preservação dos dados pessoais não estava prevista na Lei, porém, as revelações de Edward Snowden, de que o governo dos EUA estaria monitorando as comunicações do governo brasileiro incentivaram o Congresso a incluir a matéria. Neste sentido, “o MCI (Lei nº 12.965, 2014) centra-se em alguns aspectos-chave, como responsabilidade de intermediários, neutralidade de rede e regras para a guarda de registros” (p. 138).

O texto do MCI (Lei nº 12.965, 2014) explicita a necessidade de proteção à privacidade nas atividades de coleta, tratamento e armazenamento dos dados pessoais do usuário, reforçando que no Brasil as informações de comunicação são sigilosas, segundo artigo 5º, inciso XII, da Constituição Federal:

> (...) é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a Lei estabelecer para fins de investigação criminal ou instrução processual penal; (CF, 1988).

A segurança do usuário está centrada principalmente na inviolabilidade de seus dados pessoais por terceiros. Barreto Junior, Sampaio e Gallinaro (2018) pontuam que a ressalva para o compartilhamento de dados dos usuários com terceiros seriam: primeiro o prévio consentimento anterior ao tratamento (*opt-in*); e, segundo informações claras do fornecedor do serviço sobre a utilização dos dados. No caso do MCI (Lei nº 12.965, 2014), porém, não foi explicitado como seria a saída do usuário *(opt-out),* quando este indivíduo não quiser mais que o tratamento seja executado.

Konopacki e Getschko (2016) destacam que a tentativa do MCI (Lei nº 12.965, 2014) foi de minimizar o constante monitoramento do cidadão, porém, faltaram regulamentações de como isso seria feito.

No artigo 22, o MCI (Lei nº 12.965, 2014), prevê que a justiça pode requerer informações dos usuários para investigações de práticas criminosas. Amato *et al.* (2021) destacam que a Lei prevê a guarda de informações por tempo determinado, no caso das redes sociais, as informações podem ficar armazenadas por seis meses, para evitar monitoramento constante do usuário. Na preservação da privacidade do usuário a ordem “deve conter no mínimo: fundados indícios de ocorrência do ilícito; justificativa motivada da utilização dos registros solicitados para fins de investigação ou instrução probatória; e identificação do período a que se referem os registros” (p. 142).

De acordo com a Lei, o provedor só é responsabilizado pelo conteúdo de terceiros caso a justiça determine a retirada de conteúdo e a plataforma se negue a executar a ordem. A responsabilização subsidiária da plataforma, porém, é prevista em caso de divulgação de imagens de nudez ou atos sexuais sem autorização (Brasil, 2014). Santos (2020) aponta que a Lei só diferencia os provedores no artigo 18, quando menciona que os de conexão não são responsáveis por conteúdos de terceiros, portanto, esta norma acaba por aplicar-se apenas aos provedores de aplicação (redes sociais, sites, blogs).

A Medida Provisória 1.068/2021 havia incluído no MCI (Lei nº 12.965, 2014) os direitos e garantias dos usuários das redes sociais. A MP previa o acesso às informações sobre os métodos de moderação de conteúdo feitos pelas plataformas, que geraram exclusões e limitação de distribuição de publicações. Instituía a ampla defesa em caso de infração do usuário, com restituição dos conteúdos retirados e da conta, quando julgada indevida a exclusão. Indicava a exclusão de contas apenas mediante justa causa: inadimplemento de serviço pago; contas anônimas ou falsas; que ofertassem serviços piratas; ou, por determinação judicial. Impedia censura em âmbito político, ideológico, científico ou religioso.

A MP 1.068 (2021) ainda tratava de violações das normas das plataformas digitais e de conteúdos sexuais, ilegais, de incitação a crimes como tráfico, pedofilia e terrorismo, recrutamento para organizações perigosas e ainda, incitação à violência contra grupos minoritários, animais; pirataria de softwares ou roubo de dados bancários; execução de trabalho hacker. O instrumento legal trazia ainda a previsão

de notificação do usuário de infrações praticadas, com abertura de período de defesa. Porém, a medida editada em 06 de setembro de 2021 foi rejeitada pelo Senado em 16 de setembro de 2021 e praticamente não teve aplicação.

5.3.1.3 Minirreforma da Lei Eleitoral (Lei nº 13.488, 2017)

Nada foi tratado sobre campanha eleitoral no MCI (Lei nº 12.965, 2014). Para tentar preencher um pouco da lacuna legislativa, antes das eleições majoritárias de 2018, os parlamentares fizeram uma minirreforma na Lei Eleitoral (Lei 9.504, 1997), por meio da Lei 13.488, em 2017. Foram incluídos artigos que trataram da campanha online dos candidatos. Os locais na rede autorizados para ação seriam: sites, *blogs*, redes sociais e serviços de mensagem instantânea. Neste último caso, os números para o envio de mensagens precisariam estar previamente cadastrados, não podendo haver compra de banco de dados de eleitores, uma clara referência à preservação da privacidade dos usuários. A única forma de anúncio admitida na Lei foi o impulsionamento de conteúdo, contratado pelo candidato, partido ou coligação. O anúncio deveria estar devidamente identificado, para que o eleitor saiba que se trata de conteúdo pago.

Amato *et al.* (2022) sinalizam, porém, que a Lei não especifica o que seria o impulsionamento de conteúdo. Isso teria deixado de fora do escopo da legislação ações como uso de *bots*[43], para disseminação de notícias, podendo haver conteúdo mentiroso; contratação de influenciadores para fazer campanhas; e, recrutamento de empresas que fazem disparo em massa de mensagens em aplicativos de comunicação instantânea, muitas vezes por meio de compra de banco de cadastros. Esta última ação já condenada pela Lei. O perfilhamento de eleitores estaria permitido, segundo a legislação, já que esta é uma das lógicas utilizadas pelas redes sociais em impulsionamento de conteúdo.

5.3.1.4 Lei Geral de Proteção de Dados - LGPD (Lei nº 13.7096, 2018)

Em 2018, ano de eleições majoritárias no Brasil, foi aprovada a Lei Geral de Proteção de Dados (Lei 13.709/2018), que versa principalmente sobre o tratamento dos dados pessoais dos cidadãos em todos os meios de divulgação, inclusive o digital.

---

43 *Bots* é uma abreviatura para robôs, em inglês, e trata-se de um software que executa tarefas automatizadas, repetitivas e pré-definidas.

A Lei deveria ter entrado em vigor em 2020, porém, por conta da pandemia de Covid-19, teve sua *vacancis legis*[44] estendida até 2021. Para Fornasier e Knebel (2021), a LGPD (Lei Nº 13.7096, 2018) trouxe segurança jurídica ao ordenamento brasileiro, oferecendo o ambiente seguro para inovação às empresas, ao mesmo tempo que reiterou o óbvio: o cidadão é, e sempre foi, o titular de seus dados.

A Lei foi amplamente discutida, com consultas públicas online e apresentada pelo executivo em 2014. Até a aprovação foram mais 11 audiências públicas e dois seminários internacionais que congregaram legisladores, acadêmicos, setor produtivo e sociedade civil. Finkelstein e Finkelstein (2019) posicionam a aprovação da LGPD (Lei Nº 13.7096, 2018) no contexto da revelação ao mundo do caso da Cambridge Analytica, que usou dados dos usuários para manipular campanhas para a aprovação do Brexit na Inglaterra e as eleições à presidência estadunidense de 2016 (tema detalhado no capítulo 2). Além disso, soma-se ao período a entrada em vigor na Europa do Regulamento Geral sobre Proteção de Dados (RGPD), que tratava da mesma matéria (tema da próxima seção). E, ainda, a tentativa do Brasil de entrar para a OCDE. A Organização tem uma política de tratamento de dados desde a década de 1980, e a falta de um instrumento legal único que tratasse do assunto era visto como lacuna do arcabouço legal brasileiro.

Semelhantemente ao MCI (Lei nº 12.965, 2014), a LGPD (Lei Nº 13.7096, 2018) centra seus princípios nos direitos humanos, autodeterminação, liberdade tanto de expressão como informação e opinião, inviolabilidade da vida privada, preservando desenvolvimento econômico, tecnológico e a livre iniciativa. Capanema (2020) destaca que autodeterminação informativa nada mais é que a decisão do titular de saber quais dados serão utilizados, como e por quanto tempo. Antes mesmo da entrada em vigor, Sêmola e Blum (2021) pontuaram que havia na justiça mais de 600 processos referentes à LGPD (Lei nº 13.709/2018), já que ela impacta transversalmente todas as áreas do direito e da economia.

Como a Lei trata de questões técnicas, uma seção foi designada para a definição dos termos utilizados, como demonstrado no Quadro 12.

---

44 *Vacancis Legis* é um termo em latim, que compreende o período de publicação de uma lei e sua entrada em vigência.

Quadro 12 – Termos e definições da LGPD (Lei nº 13.7096, 2018) sobre tratamento de dados

TERMO	DEFINIÇÃO ESTABELECIDA EM LEI
Dado	Qualquer informação que pode identificar o cidadão
Dado sensível	Referente à identificação de raça, credo, ideologia política, filosófica ou orientação sexual
Dado anonimizado	Aqueles que não permitem identificação
Banco de dados	Estrutura onde as informações são armazenadas
Titular	Proprietário dos dados;
Controlador	Aquele que toma as decisões de tratamento dos dados
Operador	Pessoa que executa o tratamento
Encarregado	Pessoa que serve de ponte entre usuário e os demais componentes deste sistema
Agentes de tratamento	Controlador e operador
Tratamento	Toda e qualquer ação executada a partir dos dados
Anonimização	Utilização de técnica para impedir identificação
Consentimento	Manifestação de livre vontade
Bloqueio	Suspensão de tratamento
Eliminação	Exclusão de dados armazenados
Transferência internacional de dados	Transferência de dado para país ou organização da qual o brasil seja membro
Uso compartilhado de dados	Compartilhamento de tratamento para cumprimento de medida legal de entes públicos ou privados
Relatório de impacto à proteção de dados pessoais	Relatórios de tratamento que podem gerar riscos às liberdades civis e aos direitos fundamentais
Órgão de pesquisa	Entidade sem fins lucrativos que faça pesquisa histórica, científica, econômica ou estatística
Autoridade nacional de dados pessoais (ANPD)	Órgão administrativo que zela pelo implemento e fiscalização da Lei

Fonte: Elaborado pela autora com base na LGPD (Lei nº 13.709/2018)

A LGPD (Lei Nº 13.7096, 2018) ainda estabelece os princípios que devem ser usados no tratamento dos dados como finalidade, adequação, necessidade, livre acesso, transparência, não discriminação e segurança. Em seu artigo 7º, a Lei estabelece as bases legais para o tratamento, que precisa ser consentido

expressamente, a não ser que o dado seja público. Mesmo nestes casos, porém, os direitos do titular sobre os dados estão mantidos. Além disso, o consentimento deve prever a finalidade específica do tratamento. O instrumento legal especifica em seu art.º 18 que as empresas precisam informar o titular, dar acesso aos dados coletados, precisam ser corretas no tratamento, devem facilitar a portabilidade, eliminação, dentre outras obrigações (Caparanema, 2020).

O titular dos dados, segundo a Lei, tem direito ao acesso das informações. O requerimento de acesso deve ser feito sem custo e disponibilizado na forma que o titular escolher: impresso ou digital. Deve ser de fácil interpretação e o exercício de direito sobre os dados pode ser feito por via judicial, em caso de negativa das plataformas. A Lei prevê o mesmo rigor e detalhamento com relação ao tratamento dos dados pelo poder público. Para estabelecer prazo, porém, a Lei trouxe as determinações da Lei nº 9.507/1997 (Lei do Habeas Data) da Lei nº 9.784/1999 (Lei Geral do Processo Administrativo), e da Lei nº12.527/2011 (Lei de Acesso à Informação). O instrumento legal prevê que as empresas públicas de economia mista, como Banco do Brasil, têm o mesmo regramento das privadas.

Havia um regramento mais abrangente para que o poder público tivesse maior acesso aos dados dos cidadãos, proposto na MP 869/2019, porém, o instrumento teve vários artigos e incisos vetados, o que restringiu as possibilidades de tratamento dos dados pelo poder público. Foi instituído que a Autoridade Nacional de Proteção de Dados, ANPD, deve tratar dos casos de responsabilidade do poder público em caso de excesso no tratamento de dados dos cidadãos e pode requerer relatórios de minimização de impactos na privacidade do usuário.

Para a transferência internacional dos dados a Lei faz exigências de consentimento, previsão contratual, condições de segurança, apresentação de códigos e selos que atestem estas condições. Sêmola e Blum (2021) salientam que mais de 90 países já tratam da privacidade do usuário da internet em seus ordenamentos jurídicos. Sempre que for necessário para cooperação jurídica internacional e proteção da vida. Todas as condições devem ser atestadas pela ANPD, que pode requerer certificações ou escalar equipes de verificação. A ANPD pode exigir do controlador relatórios sobre a coleta, tratamento e armazenamento dos dados. Assim como transparência ao usuário no processo.

O tratamento de dados sensíveis (art. 11) exige ainda mais cuidado do controlador. Só pode ocorrer com consentimento específico ou se fizer parte de

cumprimento de medida judicial ou regulatória, para execução de políticas públicas, para pesquisas, proteção da vida, saúde e prevenção de crimes. Dados sensíveis de saúde só podem ser compartilhados se forem referentes a portabilidade de planos assistenciais, ou transações financeiras. Estas informações não podem ser utilizadas para exclusão de usuários dos planos. No caso de utilização de dados sensíveis para pesquisa, as entidades serão responsáveis pela segurança e anonimização dos dados.

Usuários menores de 18 anos precisam de consentimento de pais ou responsáveis para tratamento dos dados. O tratamento de dados deve ser interrompido com o encerramento da finalidade, por determinação judicial, regulatória ou ordenamento da autoridade nacional. A eliminação dos dados deve ser feita também no cumprimento de determinação judicial, regulatória ou ao final de pesquisa, transferência para terceiros, nas condições previstas em Lei, e para uso da ANPD (Brasil, 2018).

A Lei prevê a reparação de danos morais, materiais, individuais ou coletivos em caso de irregularidade no tratamento dos dados, que deve ser pago pelo controlador ou operador. Ambos respondem solidariamente em caso de dano causado por irregularidade no tratamento (Brasil, 2018). Sêmola e Blum (2021) salientam que LGPD (Lei Nº 13.7096, 2018) é uma Lei de gestão de riscos e a ANPD precisa ser enérgica na punição às empresas que violam normas jurídicas ou técnicas na proteção dos dados e causam danos morais ou materiais ao usuário. Além disso, é preciso que situações de vazamento de dados, mesmo que por atividade maliciosa de terceiros, sejam comunicadas imediatamente.

Capanema (2020) ressalva, porém, que a responsabilidade civil das plataformas pode ser excluída em caso de contribuição do titular para o vazamento dos dados, por exemplo, como uso de uma senha fraca para entrada no serviço online. E, quando houve tratamento dos dados, mas o serviço acusado não tem ligação com a ação, que seria culpa de um terceiro. As infrações, podem ser punidas com advertência ou multa de até 2% do faturamento da empresa, limitado a R$ 50 milhões, suspensão do tratamento dos dados da vítima, assim como suspensão do banco de dados da empresa por seis meses, prorrogável por igual período, proibição parcial ou total de tratar dados no Brasil.

Algumas irregularidades passíveis de punição podem ser exemplificadas como vazamentos de cadastros; recusa no atendimento dos direitos do titular, de informação

ou portabilidade; utilização de *spam* para disseminação de propaganda. A dosimetria da punibilidade depende de fatores como: quantidade de dados afetados; qual o tipo de dado (regular ou sensível); reincidência; omissão na minimização de riscos ou colaboração com a ANPD; a ausência de notificação dos usuários; utilização dos dados pessoais vazados por terceiros (Capanema, 2020). Sêmola e Blum (2021) atestam que o recado dado pela Lei é que as empresas sejam diligentes e se esforcem no sentido de protegerem os dados dos usuários, negligência pode gerar sanções e multas.

Sobre a Autoridade Nacional de Dados é importante observar o contexto em que foi criada. Inicialmente prevista na LGPD (Lei nº 13.709/2018), aprovada em agosto, a ANPD teve seus artigos vetados pelo então presidente Michel Temer (PMDB). Só em dezembro de 2018, a ANPD é criada pela MP 869/2018, convertida na Lei 13.853/19. Na versão original da Lei, a ANPD estaria sujeita ao ministério da Justiça, na versão aprovada ela fica subordinada à Presidência da República (Finkelstein; Finkelstein, 2019).

A ANPD teve sua estrutura aprovada pelo Decreto 10.474/20, quando efetivamente entrou em funcionamento. Inicialmente a ANPD era um órgão da administração pública federal direta. Em 2022, por meio da Medida Provisória 1.134, convertida na Lei 14.460/22, o Poder Executivo transformou a ANPD em entidade da administração pública federal indireta, submetida a regime autárquico especial. A ANPD é composta por: Conselho Diretor; Conselho Nacional de Proteção de Dados Pessoais e da Privacidade; Corregedoria; Ouvidoria; Procuradoria; unidades administrativas e unidades especializadas. Os cinco diretores são escolhidos pelo presidente, aprovados pelo Senado e cumprem mandato de quatro anos. Estes diretores devem atuar na proteção de dados, proposição de políticas públicas neste sentido, educação da população sobre o assunto, fiscalização e punição de irregularidades (Lei Nº 13.853, 2019).

Foi criado também o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPDPP) novamente incluído pela MP 869/2018, que foi revogada, instituído em definitivo pela Lei 13.853/2019. O Conselho congrega 23 representantes entre titulares e suplentes, que não recebem remuneração. São cinco do Poder Executivo Federal; um do Senado Federal; um da Câmara dos Deputados; um do Conselho Nacional de Justiça; um do Conselho Nacional do Ministério Público; um do Comitê Gestor da Internet no Brasil; três de entidades da sociedade civil; três de

instituições científicas, tecnológicas e de inovação; três de confederações sindicais representativas do setor produtivo; dois de entidades representativas do setor empresarial; dois de entidades representativas do setor laboral (Brasil, 2018).

5.3.1.4 Emenda Constitucional 115/22

Em 2022, a Constituição Federal (1988) recebeu a Emenda 115, reconhecendo a proteção de dados pessoais entre os direitos e garantias fundamentais, com competência privativa da União para legislar sobre o assunto. A EC 115/22 acrescentou o inciso LXXIX, ao artigo 5º, dispondo que "é assegurado, nos termos da Lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais". É importante destacar que a liberdade de expressão também está expressamente prevista no artigo 5º, inciso IV, com vedação ao anonimato, estabelecendo ainda o direito de resposta proporcional à ofensa, sem prejuízo do pagamento de indenização por dano moral ou material a quem foi vítima, no inciso V.

O artigo 5º da CF (1988) traz ainda expresso o direito à privacidade no inciso XII, reproduzido acima. Barreto Junior, Sampaio e Gallinaro (2018) reforçam que o conceito de privacidade, soma-se à intimidade do indivíduo. A intimidade estaria ligada ao que o cidadão tem de mais caro, que não quer compartilhar e o Estado tem o dever de preservar este direito. Os autores ressalvam, porém, que já preservados na CF/88, os direitos à liberdade de expressão e privacidade, teoricamente, não precisariam de uma inovação jurídica, como o Marco Civil da Internet (Lei 12.965, 2014) ou a LGPD (Lei nº 13.709/2018), apenas necessitava de cumprimento do dispositivo constitucional já referidos.

O que fica difícil é comungar direitos individuais no ciberespaço. Um exemplo disso é a identificação do IP da máquina de um usuário que cometeu um crime de injúria, calúnia ou difamação. Para que ele seja punido, é preciso estar identificado. Caso tenha assumido um pseudônimo na rede social, sua identificação da revelação do seu endereço de IP. Portanto, preserva-se o direito de expressão e para assegurar a responsabilização é preciso invadir a privacidade e localizar o autor pelo seu endereço de IP. Neste sentido, liberdade e segurança seriam inversamente proporcionais nas plataformas digitais, marcando uma evidente colisão dos direitos fundamentais previstos na CF/88 e as legislações regulatórias das plataformas digitais (Barreto Junior; Sampaio; Gallinaro, 2018).

5.3.1.5 Projetos de Lei referentes à liberdade de expressão

O deputado Gerson Peres (PP – PA) propôs, em abril de 2010, que donos de *blogs*, fórum e mecanismos similares fossem responsabilizados por crimes de calúnia, injúria e difamação de autores de comentários não identificáveis em suas postagens. O projeto de Lei nº 7131/2010 trazia a obrigatoriedade de identificação dos participantes de ambientes digitais que oferecessem ao usuário a possibilidade de interação com conteúdo. Por inferência, o PL 7131/2010 poderia ser aplicado às redes sociais digitais. De acordo com o texto, a moderação dos comentários era uma ação obrigatória a todos que dessem oportunidade a usuários de interagirem com o conteúdo.

No final de 2020, o deputado Roberto de Lucena (PODE – SP) apresentou o projeto de Lei nº 5347/2020, prevendo que a justiça eleitoral tivesse espaço no topo da *timeline* dos usuários brasileiros para mensagens com relação à organização e medidas sanitárias utilizadas durante os períodos de votação. O texto também previa a obrigatoriedade de as plataformas digitais criarem medidas de combate à desinformação, com disponibilização de canais de comunicação direta entre usuários e a justiça eleitoral, para combate de disparos de mensagens em massa e demais irregularidades. Com teor semelhante, foi apensado a esta proposta o projeto de Lei nº 5567/2020, do deputado Rubens Otoni (PT – GO).

Já o projeto de Lei nº 3700/2021, do deputado José Guimarães (PT – CE) propôs que as plataformas de mídias sociais criassem parâmetros de moderação para discurso de ódio. O texto previa a inclusão de artigo informando que as mídias sociais deveriam primar pela “promoção do bem comum, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação” (Art. 2º, VII). A notificação de usuário referente a postagem com discurso de ódio ensejaria a remoção do conteúdo em até 24 horas pela plataforma digital. Foi instituída na proposta como discurso de ódio *posts* que incitassem violência ou grave ameaça, com discriminação racial, social ou religiosa.

Fotos manipuladas por computador deveriam receber um aviso aos usuários, esta foi a proposta feita pelo deputado Airton Faleiro (PT – PA), no projeto de Lei

2762/2021. De acordo com o texto, qualquer foto veiculada em meio digital, que tiverem recebido retoque deveriam apresentar um alerta ao usuário. Além disso, as plataformas digitais deveriam abrir espaços para denúncias quando imagens retocadas não estiverem identificadas.

Em fevereiro de 2022, o deputado Marco Feliciano (PL – SP) propôs a criação de um órgão, dentro do Ministério das Comunicações, para verificar a veracidade das informações postadas em redes sociais. De acordo com o projeto de Lei nº 188/2022, o órgão teria especialistas de cada área e agiria por provocação. Após a verificação da veracidade das informações teria ação administrativa, que depois poderia se converter em criminal. O projeto não detalhou contra seria a ação, se contra o autor do material ou contra a plataforma.

A exclusão de conteúdo das redes sociais estaria sujeita à ampla defesa e ao contraditório. Esta era a proposta que foi apresentada no projeto de Lei nº 2831/2021, do deputado Capitão Alberto Neto (REPUBLIC – AM). De acordo com o texto, além de oferecer regras claras de moderação de conteúdo aos usuários, as redes sociais estariam condicionadas a aviso de ação de moderação de conteúdo, para que o autor da postagem pudesse se defender. O prazo para apresentação da defesa seria de 48 anos, com possibilidade de restauração de conteúdo excluído ou que tivesse apresentado distribuição reduzida.

Já no encerramento de 2022, o deputado Sóstenes Cavalcante (PL – RJ) apresentou o projeto de Lei nº 3046/2022, com proposta de disciplinar a exclusão ou bloqueio de contas de parlamentares em redes sociais digitais. De acordo com o texto, qualquer ação de moderação de conteúdo ou conta de membro do Congresso Nacional constituiria medida cautelar de caráter excepcionalíssimo. A ação deveria conter crime no qual o parlamentar tivesse incorrido, assim como, parecer do ministério público para consumação da moderação. A inobservância do rito poderia ocasionar multa de R$ 10 milhões à plataforma digital.

Maranhão, Campos e Guedes (2021) observam que até o momento há uma crítica severa à forma como as plataformas digitais executam a moderação de conteúdo. Faltam mecanismos efetivos de contestação, com as plataformas mantendo uma discricionariedade excessiva na moderação. Além disso, o uso de ação automatizada pode levar a um bloqueio demasiado de conteúdo, promovendo censura. O ideal seria que os Princípios de Santa Clara para moderação de conteúdo fossem de fato respeitados com a divulgação dos relatórios com números claros e de

fácil compreensão da ação moderadora; com avisos de ação visíveis tanto ao usuário, quanto a quem denunciou o conteúdo nocivo; e, por fim, com as empresas dando real oportunidade de recurso a quem sofreu a moderação, com possibilidade de revisão externa.

5.3.1.6 Projetos de Lei referentes à liberdade de expressão e segurança

Para evitar que as pessoas tomassem decisões equivocadas, o deputado Célio Silveira (PSDB – GO) apresentou o projeto de Lei nº 10919/2018, que previa a identificação de conteúdo publicitário. Ficou muito comum em um período que celebridades fossem pagas para fazer *publipots* nas redes sociais. Às vezes, nos *posts,* os produtos eram mostrados apenas como um teste de utilização, como se tivessem sido comprados ou recebidas marcas. A proposta de Silveira era de que postagens pagas fossem identificadas com *tags* visíveis.

Para evitar que menores tenham acesso a conteúdo previsto para adultos, o deputado Dagoberto Nogueira (PDT – MS) apresentou o projeto de Lei nº 3993/2020. De acordo com o texto, para terem acesso às plataformas digitais os usuários seriam obrigados a apresentarem documento de identificação válido no território nacional. Desta forma, as plataformas digitais estariam obrigadas a impedir que menores de 18 anos tivessem acesso a conteúdo destinado a adultos.

A preocupação com conteúdo direcionado a crianças e adolescente também estava prevista no projeto de Lei nº 2557/2022, dos deputados Tiago Andrino (PSB – TO) e Felipe Carreras (PSB – PE). O texto previu que os provedores de aplicação de internet deveriam prever o desenvolvimento intelectual e segurança dos usuários menores de idade. O projeto de Lei instituiria a criação da Política Nacional de Proteção Digital das Crianças e Adolescentes (PNPD), que teria o objetivo de evitar a exposição de menor a conteúdo impróprio, com previsão de reparação a possíveis danos causados. O poder executivo traria os parâmetros sobre o conteúdo impróprio, caberia às plataformas seguir estas balizas.

Para que o conteúdo impróprio não chegasse aos menores, caberia às plataformas digitais encontrarem ferramentas de bloqueio. Dentro das previsões também foi estabelecido que as plataformas teriam de criar ferramentas de controle parental, assim como mecanismos de identificação que não permitiriam acesso de menor a conteúdo impróprio. A aquisição de produtos também exigiria identificação

para evitar que menores incorressem em transações financeiras de forma fraudulenta. O desrespeito às normas geraria sanções que iriam desde advertência, até multa, suspensão ou impedimento de exercício da atividade no Brasil (2557/2022).

5.3.1.7 Projetos de Lei referentes à privacidade

Em 2016, a senadora Vanessa Grazziotin (PcdoB – AM) apresentou a proposta do projeto de Lei nº 347/2016, que previa a alteração da Lei nº 12.965, conhecida como Marco Civil da Internet (Lei 12.965, 2014). A senadora propunha que seria necessário que houvesse consentimento prévio do usuário para fazer o cadastramento e envio de convites para participação em redes e mídias sociais, assim como em grupos, páginas, comunidades e similares. A parlamentar chamava a atenção para a necessidade de se ater à forma como as mídias sociais estariam angariando novos membros, com acesso a listas de contatos, com aberturas de perfis, sem o devido consentimento do usuário. Além disso, o usuário pode ser incluído em páginas e grupos privados com conteúdo violento ou pornográfico, sem prévio consentimento. Estas ações não teriam sido contempladas pelo Marco Civil da Internet (Lei 12.965, 2014).

Para Fornasier e Knebel (2021), a cidadania digital depreende que as pessoas tenham um conhecimento mínimo de tecnologia para compreender o que de fato estão cedendo às plataformas digitais quando dão seu consentimento para o tratamento dos dados. A propriedade sobre os dados é uma característica da sociedade da informação, que está cada vez mais dependente da tecnologia em seu modo de vida. Por isso, a regulação de como as informações serão transacionadas precisa existir como base desta sociedade.

5.3.1.8 Projetos de Lei referentes à privacidade e segurança

Apresentado em agosto de 2020, o projeto de Lei nº 4120/2020, tratava da utilização de algoritmos pelas plataformas digitais para influenciar seus usuários na tomada de decisões. De acordo com a proposta do deputado Bosco Costa (PL – SE), seria ilícito para as plataformas digitais a prática discriminatória ou abusiva, utilizando as Leituras algorítmicas aplicadas ao comportamento do usuário. Além disso, seria as plataformas digitais precisariam agir com princípios da boa-fé, transparência, responsabilidade social, segurança, respeitando valores éticos e morais, direito à

privacidade e à intimidade dos cidadãos e os direitos humanos e à democracia, somados à legislação de Tratados Internacionais dos quais o Brasil é signatário.

A proposta obrigaria as plataformas a emitirem relatórios sobre impacto da ação algorítmica e comunicar os usuários sobre suas atividades que utilizam sistema de decisão automatizada. Além disso, usuários deveriam ser instruídos sobre a utilização de tais sistemas de decisão automatizadas das plataformas digitais. As penalidades para os infratores iriam de advertência, multa, suspensão e até de atividades no país (PL 4120/2020).

Em novembro de 2022, o deputado João Maia (PL – RN) apresentou o projeto de Lei nº 2768/2022, que propunha uma série de obrigações que as plataformas digitais deveriam seguir para operação no Brasil. Entre as principais normas estavam previstas normas de transparência de dados e fornecimento de informações à Agência Nacional de Telecomunicações; tratamento isonômico e não-discriminatório aos usuários; acesso facilitado ao usuário para portabilidade de dados. O projeto propõe a criação de um fundo de fiscalização das plataformas digitais, o FisDigi. Todos os valores aferidos com aplicação de multa iriam para este fundo, assim como uma contribuição anual de 2% da receita operacional bruta da empresa. A Lei ainda tem algumas provisões a respeito de liberdade econômica e livre inciativa que ficam fora do escopo desta tese.

5.3.1.9 Projetos de Lei referentes à segurança

Para evitar a prática de crime de preconceito de raça, cor, etnia, religião ou procedência nacional, o deputado Ângelo Agnolin (PDT – TO) apresentou o projeto de Lei nº 1468/2011, para obrigar as plataformas digitais a incluírem em seus termos de adesão aos serviços digitais o aviso de que postagens discriminatórias seriam consideradas prática criminal. Ficaria o provedor obrigado a retirar do ar tais postagens e fornecer ainda material probatório para a instrução processual, assim como meios de identificação do usuário que praticasse o crime.

O direito do consumidor brasileiro foi o foco do projeto de Lei nº 4565/2012, apresentado pelo deputado Professor Victório Galli (PMDB – MT). Segundo o texto da proposta, qualquer plataforma digital ou aplicativo de internet deveria redigir seus contratos de oferta de serviço de acordo com a legislação brasileira. Além disso, qualquer ação, inclusive de arbitragem, deveria ser feita em território nacional.

O uso das redes sociais para aviso da ocorrência de blitz policial seria considerado crime, caso o projeto de Lei nº 5596/2013, do deputado Major Fábio (DEM – PB), fosse aprovado. A proposta trazia ainda a obrigatoriedade das plataformas digitais de retirarem tal conteúdo do ar, sob pena de pagamento de multa de R$ 50 mil por ocorrência denunciada.

Com foco na saúde e prevenção do comportamento adicto às redes sociais e internet foi apresentado o projeto de Lei nº 2498/2015, do deputado Aureo Ribeiro (SD – RJ). O parlamentar trouxe à discussão proposta de que os provedores de serviços de internet em conjunto, ou separadamente, abrissem e mantivessem centros de prevenção e tratamento para pessoas viciadas em redes sociais. Os centros teriam a função de orientar usuários para evitar uso compulsivo da internet. Cada unidade da federação deveria ter ao menos um centro de tratamento e orientação.

De acordo com o texto, o uso compulsivo de internet seria considerado quando o indivíduo perdesse a noção de tempo na utilização dos serviços, ignorando, inclusive, impulsos básicos; irritabilidade ou intolerância em abstinência do uso dos serviços digitais; além de comportamento antissocial, baixo desempenho, isolamento e fadiga. Para estes indivíduos os tratamentos deveriam prever ferramentas de organização e gestão do tempo; instrução sobre malefícios e benefícios da internet; controle de emoções; e, melhoria de comunicação interpessoal e habilidades sociais. Com combate contra depressão, ansiedade, solidão e estresse (2498/2015).

Vários foram os instrumentos legislativos que tipificaram a conduta de incentivo à automutilação e ao suicídio nas redes sociais como crime, porém, foi o projeto de Lei nº 7460/2017, da deputada Leandre Dal Ponte (PV – PR), que propôs a obrigatoriedade de as plataformas digitais retirarem este tipo de conteúdo de seus ambientes digitais. Além disso, tipificou como crime a não exclusão de material desta natureza pelos provedores de serviços digitais depois de terem sido notificados. Já o projeto de Lei nº 7917/2017, do deputado Vítor Valim (PMDB – CE)**,** trouxe a obrigatoriedade de que em caso de busca de informação sobre automutilação e suicídio, as plataformas digitais fossem obrigadas a divulgar o número, 141, do Centro de Valorização à Vida (CVV). Caberia ao poder público criar o código de boas práticas, com palavras-chaves para divulgação da mensagem de alerta.

Anos mais tarde, a deputada Rejane Dias (PT – PI), apresentou a proposta do projeto de Lei nº 3496/2019, que também obrigaria as plataformas digitais a retirarem conteúdo de automutilação e incentivo a suicídio do ar. Além disso, a proposta previa

a obrigatoriedade de instalação de um canal para denúncia de conteúdo desta natureza, com notificação ao denunciante de todos os passos tomados a partir da notificação feita à plataforma. Conteúdo denunciado e não removido geraria multa de R$ 100 mil à plataforma.

Ainda na busca pela segurança de crianças e adolescentes, o deputado Roberto Alves (PRB – SP) apresentou os projetos de Lei 2184 e 2185/2019, que tratava da obrigatoriedade das plataformas digitais de emitirem avisos de proibição de propagação de imagens de exploração sexual de menores, já que a prática consiste em crime tipificado no Brasil. De acordo com a proposta, os avisos educativos deveriam ser exibidos aos usuários durante no mínimo 15 segundos a cada acesso feito à rede social.

Ainda com relação à segurança infantil, o deputado Alexandre Frota (PSDB – SP) apresentou o projeto de Lei nº 4801/2020, que previa a obrigatoriedade às redes sociais de publicarem mensagem sobre os malefícios do trabalho infantil.

Para evitar que ataques massivos a pessoas fossem publicizados na mídia, o deputado Coronel Tadeu (PSL – SP) apresentou o projeto de Lei nº 2463/2019. A proposta previa uma proibição, inclusive de plataformas digitais, de divulgação de imagens de situações de ataques massivos a pessoas. Estariam proibidas também a divulgação de nomes e demais dados pessoais dos envolvidos no crime, até mesmo as vítimas. A desobediência à norma geraria multa de R$ 1 milhão para as plataformas digitais e R$ 100 mil para usuários que fizessem os *posts*.

No início de 2022, o deputado Marcelo Ramos (PL – AM) introduziu na Câmara o projeto de Lei nº 397/2022, que obrigaria empresas de serviços digitais, mesmo com sede no exterior, que tivessem representante legal no País. De acordo com o texto da proposta, o objetivo seria assegurar o cumprimento de Leis, “receber citações, intimações ou notificações, em quaisquer ações judiciais e procedimentos administrativos, principalmente fiscais, e responder perante órgãos e autoridades governamentais (Art. 2º). As informações sobre tal representante deveriam ter acesso facilitado no site da empresa, com guarda de conteúdo dos usuários brasileiros para situações previstas em cumprimento de Leis. Agir em desacordo com a Lei bloquearia o serviço no País. Proposta idêntica fez o deputado Luciano Bivar (UNIÃO – PE) com o projeto de Lei nº 630/2022.

5.3.1.10 Projetos de Lei referentes à liberdade de expressão, privacidade e segurança

Entre os anos de 2020 e 2022 tramitou no Congresso o projeto de Lei 2630/2020, que instituiria a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet, apresentado pelo senador Alessandro Vieira (CIDADANIA – SE). O PL abarca regramento para plataformas de mídias sociais, serviços de busca e aplicativos de mensagens instantâneas via internet, com mais de 10 milhões de usuários.

Ao todo, o PL 2630/2020 teve 73 projetos de Lei apensados até o final de 2022, data limite de levantamento desta pesquisa. As propostas legislativas associadas a ele vão ser apenas listadas para conhecimento, posteriormente, o projeto de Lei será analisado em maiores detalhes. Os projetos apensados serão demonstrados de acordo com os parâmetros previstos nesta tese, que verificam normas referentes a liberdade de expressão, privacidade e segurança do usuário, utilizando os subtemas em que foram incluídos:

1- Liberdade de Expressão:

- Tratam do rito de moderação de conteúdo e notificação de usuário:
    - PL 2602/2019 – proposto pelo deputado Luis Miranda (DEM – DF)
    - PL 283/2020 – proposto pelo deputado Cássio Andrade (PSB – PA)
    - PL 3119/2020 – proposto pelo deputado Mário Negromonte Jr. (PP – BA)
    - PL 3395/2020 – proposto pela deputada Bia Kicis (PSL – DF), Carla Zambelli (PSL – SP), General Girão (PSL – RN)
    - PL 3573/2020 – proposto pelos deputados Luiz Philippe de Orleans (PSL – SP) e Bragança e Carla Zambelli (PSL – SP)
    - PL 2883/2020 – proposto pelo deputado Filipe Barros (PSL – PR)
    - PL 127/2021 – proposto pelo deputado Nelson Barbudo (PSL – MT)
    - PL 356/2021 – proposto pelo deputado General Girão (PSL – RN)
    - PL 388/2021 – proposto pelo deputado Carlos Jordy (PSL – RJ)
    - PL 1743/2021 – proposto pelo deputado Giovani Cherini (PL – RS)
    - PL 1897/2021 – proposto pelo deputado Alexandre Frota (PSDB – SP)
- Tratam de conteúdo de desinformação e fraude:
    - PL 6812/2017 – proposto pelo deputado Luiz Carlos Hauly (PSDB – PR)
    - PL 7604/2017 – proposto pelo deputado Luiz Carlos Hauly (PSDB – PR)

- PL 8592/2017 – proposto pelo deputado Jorge Côrte Real (PTB – PE)
- PL 9554/2018 – proposto pelo deputado Pompeo de Mattos (PDT – RS)
- PL 9761/2018 – proposto pelo deputado Celso Russomanno (PRB – SP)
- PL 9838/2018 – proposto pelo deputado Arthur Oliveira Maia (PPS – BA)
- PL 9884/2018 – proposto pelo deputado Fábio Trad (PSD – MS)
- PL 9931/2018 – proposto pelo deputado Erika Kokay (PT – DF)
- PL 2601/2019 – proposto pelo deputado Luis Miranda (DEM – DF)
- PL 200/2019 – proposto pelo deputado Roberto de Lucena (PODE – SP)
- PL 241/2019 – proposto pelo deputado Júnior Ferrari (PSD – PA)
- PL 1974/2019 – proposto pelo deputado Reginaldo Lopes (PT – MG)
- PL 3857/2019 – proposto pelo deputado Jaqueline Cassol (PP – RO)
- PL 2854/2020 – proposto pela deputada Maria do Rosário (PT – RS), Luizianne Lins (PT – CE), Rui Falcão (PT – SP)
- PL 693/2020 – proposto pelo deputado Alexandre Padilha (PT – SP)
- PL 705/2020 – proposto pelo deputado Célio Studart (PV – CE)
- PL 1394/2020 – proposto pelo deputado Zé Vítor (PL – MG)
- PL 988/2020 – proposto pelo deputado Alexandre Frota (PSDB – SP)
- PL 2196/2020 – proposto pelo deputado Alexandre Frota (PSDB – SP)
- PL 3307/2020 – proposto pelo deputado Alexandre Frota (PSDB – SP)
- PL 1258/2020 – proposto pelo deputado Luis Miranda (DEM – DF)
- PL 1941/2020 – proposto pelo deputado Wilson Santiago (PTB – PB)
- PL 2389/2020 – proposto pelo deputado Rejane Dias (PT – PI)
- PL 808/2020 – proposto pelo deputado José Guimarães (PT – CE)
- PL 2844/2020 – proposto pelo deputado Joseildo Ramos (PT – BA)
- PL 3222/2020 – proposto pelo deputado Frei Anastacio Ribeiro (PT – PB)
- PL 2790/2020 – proposto pelo deputado José Nelto (PODE – GO)
- PL 2516/2022 – proposto pelo deputado José Nelto (PODE – GO)
- PL 4134/2021 – proposto pelo deputado Carlos Bezerra (MDB – MT)
- PL 1923/2021 – proposto pelo deputado Alexandre Frota (PSDB – SP)
- PL 1001/2021 – proposto pelo deputado Helder Salomão (PT – ES), Paulo Teixeira (PT – SP), Túlio Gadêlha (PDT – PE)

- Tratam de conteúdo de exploração sexual e violência:
  - PL 1590/2021 – proposto pelo deputado Renata Abreu (PODE – SP)

2- Privacidade

- Direito ao esquecimento:
    - PL 1676/2015 – proposto pelo deputado Veneziano Vital do Rêgo (PMDB – PB)
    - PL 2712/2015 – proposto pelo deputado Jefferson Campos (PSD – SP)
    - PL 10860/2018 – proposto pelo deputado Augusto Carvalho (SD – DF)
    - PL 346/2019 – proposto pelo deputado Danilo Cabral (PSB – PE)
    - PL 5776/2019 – proposto pelo deputado Afonso Mota (PDT – RS)
    - PL 4418/2020 – proposto pelo deputado David Soares (DEM – SP)
- Estabelece obrigatoriedade de identificação do usuário:
    - PL 9647/2018 – proposto pelo deputado Heuler Cruvinel (PSD – GO)
    - PL 3389/2019 – proposto pelo deputado Fábio Faria (PSD – RN)
    - PL 4925/2019 – proposto pelo deputado Moises Rodrigues (MDB – CE)
    - PL 5260/2019 – proposto pelo deputado Nereu Crispim (PSL – RS)
    - PL 6351/2019 – proposto pelo deputado Luis Miranda (DEM – DF)
    - PL 437/2020 – proposto pelo deputado Alexandre Frota (PSDB – SP)
    - PL 2284/2020 – proposto pelo deputado Alexandre Frota (PSDB – SP)
    - PL 517/2020 – proposto pelo deputado José Medeiros (PODE – MT)
    - PL 3044/2020 – proposto pelo deputado Paulo Ramos (PDT – RJ)
    - PL 2763/2020 – proposto pelo deputado Marcelo Brum (PSL – RS)
    - PL 3627/2020 – proposto pelo deputado Nereu Crispim (PSL – RS)
    - PL 2989/2021 – proposto pelo deputado Marx Beltrão (PSD – AL)
- Prevê direito de atualização de informações pessoais a pedido do usuário:
    - PL 2390/2021 – proposto pelo deputado Emanuel Pinheiro Neto (PTB – MT)
- Proíbe apresentação de resultados a consulta de nomes de policiais absolvidos em ações criminais:
    - PL 475/2020 – proposto pelo deputado Capitão Alberto Neto (REPUBLIC – AM)
- Estabelecem regras de tratamento e portabilidade de dados
    - PL 5959/2019 – proposto pelo deputado Luizão Goulart (REPUBLIC – PR)

- PL 1772/2021 – proposto pelo deputado Luiz Philippe de Orleans e Bragança (PSL – SP)
- PL 3366/2021 – proposto pela deputada Rejane Dias (PT – PI)

3- Segurança do usuário

- Tratam de crime contra a segurança nacional:
  - PL 9533/2018 – proposto pelo deputado Francisco Floriano (DEM – RJ)
  - PL 2060/2021 – proposto pelo deputado Altineu Côrtes (PL – RJ)

4- Apresenta intersecção entre liberdade de expressão, privacidade e/ou segurança

- Tratam de parâmetros de transparência, moderação de conteúdo e tratamento de dados:
  - PL 3063/2020 – proposto pelo deputado Felipe Rigoni (PSB – ES), Tabata Amaral (PDT – SP)
  - PL 3144/2020 – proposto pelo deputado Joice Hasselmann (PSL – SP)
  - PL 143/2022 – proposto pelo deputado Coronel Armando (PSL – SC)
  - PL 714/2022 – proposto pelo deputado Nereu Crispim (PSL – RS)
  - PL 836/2022 – proposto pelo deputado Eduardo Bolsonaro (PL – SP)

Vieira (2023) apontou que inicialmente a intenção do projeto era combater contas falsas, publicidade e redes de transmissão não divulgadas, que são as grandes ferramentas de disseminação de desinformação. Porém, não havia no projeto qualquer menção à moderação de conteúdo. No princípio a ideia era poder identificar quem tivesse cometido qualquer tipo de crime na rede, já que a CF garante a liberdade de expressão, mas veda o anonimato. Com o andamento do projeto e a atual redação, o PL também trouxe normas com relação à moderação de conteúdo.

Logo no início do texto há uma ressalva sobre a proteção dos direitos fundamentais previstos no artigo 5º, inciso IX, da CF, reiterando que “é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença”. São nove os princípios do PL 2630 (2020), que incluem: liberdade de expressão e de imprensa; preservação dos direitos de personalidade, dignidade, honra e privacidade; respeito às preferências políticas e visão de mundo; preservação da pluralidade e democracia; segurança dos sistemas informacionais; promoção do conhecimento; acesso aos meios de comunicação e à informação; proteção dos consumidores; transparência na veiculação de conteúdo pago.

Maranhão, Campos e Guedes (2021) salientam os objetivos propostos pelo PL, que inclui o fortalecimento da democracia no combate à desinformação e contas inautênticas, defendendo a liberdade e rechaçando a censura, buscando dar maior transparência ao ambiente das redes sociais, na moderação de conteúdo, assim como clareza em anúncios. Os autores relembram os parâmetros do Princípio de Manila, para a responsabilização dos intermediários que buscam incentivar "a inovação, respeitando os direitos dos usuários, de acordo com a Declaração Universal dos Direitos Humanos, o Pacto Internacional sobre Direitos Civis e Políticos e os Princípios Orientadores das Nações Unidas sobre Negócios e Direitos Humanos" (p. 13).

O texto do PL 2630 (2020) propõe aos provedores que vedem o funcionamento de contas automatizadas, que não forem identificadas; exige a identificação de todos os conteúdos impulsionados, inclusive os compartilhados; estabelece a necessidade de conferir acesso não discriminatório. Com relação à transparência, exige que os termos de uso sejam feitos em português e prima pelo respeito à legislação nacional visando o acesso à informação, liberdade de expressão e livre concorrência. O texto ressalta que o tratamento dos dados dos usuários deve respeitar o regramento imposto pela LGPD (Lei nº 13.709/2018). Para as plataformas de mídias sociais reitera que são necessários critérios claros para remoção de conteúdo, ressalvando os segredos comercial e industrial do setor.

O PL 2630 (2020) institui a elaboração de relatórios que devem ser feitos e disponibilizados aos usuários sobre intervenção em contas como remoção de conteúdo, redução de alcance, cancelamento de contas e outras ações que restringem a liberdade de expressão. Estes documentos devem conter número de usuários das redes que acessaram do Brasil; número de medidas aplicadas conforme autorregulação dos provedores, em cumprimento à Lei, e em cumprimento à medida judicial, segmentada; número de pedidos de revisão apresentados; detalhes sobre equipes envolvidas na moderação ou sistema automatizado para esta finalidade; número de medidas de sinalização; e, revisões semestrais de termos de uso e justificativa de eventuais mudanças.

Curzi *et al.* (2021) criticam a falta de uma metodologia ou modelo determinado para a elaboração dos relatórios, dificultando a fiscalização de possíveis falhas. Vieira (2023) informou que na elaboração do PL era preciso estabelecer um órgão que recebesse os relatórios das empresas, para que checar a conformidade com a Lei. O órgão poderia ser o CGI, ANATEL, ou qualquer outro de caráter administrativo apenas,

porém, a ideia majoritária era de que se criasse uma outra entidade com esta tarefa. Para isso, Veira sugeriu que se criasse uma entidade paritária, fora do Executivo, para evitar viés ideológico na tomada de decisão e tarefa de fiscalização, e que contasse com a participação da sociedade civil.

De acordo com o PL, as informações devem ser disponibilizadas publicamente e com linguagem acessível. Após a aplicação de sanções, usuários devem ser comunicados sobre a natureza da medida aplicada, fundamentação dentro das políticas da rede social ou da Lei, que embasam a decisão, dar prazo e estabelecer procedimentos de defesa, disponibilizar canal para o recurso e responder à solicitação de forma rápida e fundamentada. Caso a medida da rede social tenha sido equivocada, ela deve dar publicidade ao erro (PL 2630, 2020). Curzi *et al.* (2021) notam que faltam diretrizes de proporcionalidade e razoabilidade nas punições de usuários e uma determinação do prazo para resposta das plataformas em caso de recurso.

A publicidade em *posts* deve ser identificada, com a identificação do pagador pelo anúncio. Os usuários devem ter acesso a todo conteúdo impulsionado com o qual tiveram contato pelos últimos seis meses. As propagandas eleitorais devem estar sinalizadas, com valor gasto na campanha, identificando o anunciante por CNPJ ou CPF, tempo de veiculação, audiência contratada, técnicas de perfilhamento, endereço eletrônico e cópia das mensagens de quem autorizou. Os provedores são responsáveis pela comprovação da identidade do pagador do impulsionamento por meio de documentos válidos. Comercialização de anúncios de empresas sediadas no exterior deve ser regida pela filial brasileira (PL 2630, 2020). Viera (2023) destaca que o PL proíbe o perfilhamento algorítmico de menores para oferta de produtos e serviços.

De acordo com o PL 2630 (2020) contas de entidades ou entes públicos, como políticos, serão consideradas institucionais e não poderão sofrer restrição de visualização. Caso sofram alguma intervenção, por parte dos provedores, estas contas podem requerer retirada de bloqueio por via judicial. Em medidas de restrição de liberdade de expressão nestas contas de interesse público, os provedores serão obrigados a colocar mensagem sobre a ação feita e sua fundamentação. Os agentes políticos ou servidores públicos, que utilizam suas contas para divulgação da atuação profissional, com mais de uma conta devem submeter apenas uma a este regramento, comunicando o corregedor de sua área sobre qual é o perfil profissional. Pela

proposta, esta lista das corregedorias seria atualizada a cada posse de mandato e comunicada à rede social em até 60 dias. A imunidade parlamentar estende-se à rede social.

O PL 2630 (2020) veda o recebimento de monetização de conteúdo para agentes políticos, em cargos eletivos, membros das Forças Armadas, e militares de Estados. Os valores, nestes casos, se existirem, devem ser revertidos à União. Os gastos com impulsionamento feito por órgãos públicos deve constar em seus portais de transparência. Além disso, é vedada a contratação de publicidade por entes públicos em provedores que incitam crimes ou discriminação de qualquer natureza. Os recursos investidos em publicidade devem ser discriminados por meio escolhido.

As sanções propostas pelo PL 2630 (2020) são: advertência; multa de 10% sobre o faturamento, ou R$ 10 a R$ 1000 por usuário cadastrado, limitada a R$ 50 milhões; suspensão ou proibição da atividade no país. Se for empresa estrangeira, a filial responde solidariamente. As sanções serão aplicadas mediante gradação de infração, reincidência, capacidade econômica. Os valores de multas serão destinados ao Ministério da Educação.

O crime previsto no PL (art. 36) seria o de promover ou financiar disseminação de mensagens que contenham fato inverídico, que possa comprometer o processo eleitoral, ou causar dano físico a alguém. O crime teria pena de 1 a 3 anos de reclusão, mais multa (PL 2630/2020). Curzi *et al.* (2021) apontam que o Direito Penal não seria o caminho ideal para lidar com o problema, visto o princípio da subsidiariedade e pelo risco de influência política sobre o tema.

O Comitê Gestor da Internet seria o órgão responsável pela elaboração de um código de conduta aos provedores. Poderia, para isso, solicitar informações sobre as metodologias utilizadas para intervenção em contas e conteúdos gerados, no intuito de elaborar políticas públicas de manutenção da liberdade de expressão (PL 2630, 2020). Curzi *et al.* (2021) notam que a redação do PL não deixa claro quais seriam as regras a serem elaboradas pelo CGI e muito menos sobre possíveis sanções às plataformas caso não cumpram as recomendações.

O PL 2630 (2020) propõe uma autorregulação regulada às plataformas. A indicação seria de que os provedores criassem instituições de recebimento de denúncias de conteúdo ou contas, assim como, que promovessem a revisão conjunta de decisões já tomadas; e, trabalhassem em parceria com empresas de telefonia, para checagem de autenticidade de contas. A instituição teria uma natureza associada, de

acordo com o Código Civil Brasileiro. Maranhão, Campos e Guedes (2021) notam que na autorregulação conta-se com o *know how* da plataforma com relação a seu setor; já na regulação, muitas vezes falta celeridade na dinâmica de ação pela mudança constante da tecnologia. O ideal, neste sentido, é que o Estado elabore parâmetros para a confecção das normas de autorregulação das plataformas.

Para Amato *et al.* (2022), a autorregulação regulada seria uma das principais inovações da Lei, pois “trata-se de formas jurídicas que se distanciam do sistema político estatal e se implantam dentro da dinâmica autorreferente de outros sistemas (no caso, o sistema dos meios de comunicação digitais” (p. 159). Ao Estado caberia estabelecer parâmetros, para a decisão que seria tomada na esfera privada. A Alemanha e a própria União Europeia já tratam do assunto nestes termos. As plataformas voltam a ter protagonismo na moderação de conteúdo, e a crítica fica centrada no tolhimento à liberdade de expressão. A autorregulação regulada seria uma maneira de tornar legal a maneira opaca como as plataformas digitais vêm moderando conteúdo.

Os provedores precisariam contar com representantes jurídicos no Brasil. Todo o conteúdo jornalístico utilizado pelos provedores receberia remuneração. Estão contemplados no texto os veículos de mídia e produtores de notícia com no mínimo 12 meses de trabalho e editor no Brasil. O PL 2630 (2020) prevê a revisão da Lei em cinco anos após a aprovação.

Numa investigação feita por pesquisadores da Fundação Getúlio Vargas (FGV), sobre a discussão virtual da regulação das plataformas digitais, postagens no Twitter passaram por um monitoramento no início de 2022. Foram analisadas 1,14 milhão de menções sobre o tema entre 1º de fevereiro a 06 de abril. O levantamento apontou que 54,6% dos perfis analisados eram contrários ao PL, outros 20,49% favoráveis. As manifestações contrárias ao PL tiveram 82,11% de interação, enquanto as favoráveis somaram 9,84% de engajamento (Ruediger *et al.*, 2022).

De acordo com Bia Barbosa (2022), o PL das Fake News não obteve o quórum de dois terços em uma votação na câmara dos deputados, o que impediu que uma audiência pública sobre o projeto fosse realizada. Com isso, o presidente da casa, Arthur Lira (PP), decidiu pela criação de uma comissão especial para a discutir a matéria, com emissão de pareceres, para posteriormente ser discutida na câmara. O texto atual do projeto trata de uma transparência maior das plataformas, regras para a moderação de conteúdo, com estabelecimento de regras de ação das plataformas

e reação dos usuários, caso se sintam insatisfeitos, inclusive, no quesito reparação em caso de prejuízo. Além disso, o projeto estabelece que conteúdo impulsionado precisa ser claro quanto a esta informação, assim como de contas automatizadas.

5.3.2 Mecanismos legais dos EUA

Nos Estados Unidos, a agenda regulatória esteve presente desde o início da internet, na década de 1990, porém, foram considerados projetos introduzidos nas casas legislativas a partir de 2006, quando o Twitter foi lançado. Entre os resultados, foram selecionados apenas os projetos que tratavam exclusivamente de regulação das plataformas digitais dentro do escopo proposto para esta pesquisa, que analisa as regras prevendo a manutenção de direitos fundamentais dos cidadãos em sociedades democráticas que incluem liberdade de expressão, privacidade e segurança do usuário.

Estas normas passaram por quatro filtros: casa legislativa em que foram apresentadas, autores, data de introdução e resumo do tema em discussão. No cruzamento de dados foi possível perceber que alguns projetos eram minimamente modificados em novas legislaturas e novamente apresentados pelos mesmos autores, ou então, por parlamentares do mesmo partido. Os projetos de Lei que serão analisados são apresentados no Quadro 13, com a organização a partir da data da primeira ou única introdução na Câmara, que estão identificados com as iniciais H. R. (House of Representative) e Senado, representado com a letra S. (Senate). Estará à frente o local onde a proposta foi apresentada inicialmente.

Quadro 13 – Projetos de Leis de regulação propostos nos EUA de 2006 a 2022

MECANISMO LEGAL	AUTORES	DATAS	RESUMO DA PROPOSTA
S.215 (2007) / H.R.5353 (2008) - Internet Freedom Preservation Act	Byron Dorgan (PD – ND) Edward J. Markey (PD – MA)	09/01/2007 12/02/2008	Exige que as plataformas digitais ofereçam serviço com garantia de segurança de rede e evitem ação discriminatória na distribuição de conteúdo.
S.1625 - Counter Spy Act	Mike Pryor (PD – AR)	14/06/2007	Proíbe a instalação de software de captação de dados em computador alheio, sem autorização do usuário.
H.R.3850 - Responsible and Effective Solutions for Children	Christopher Carney	16/10/2007	Traria às plataformas digitais a imunidade de responsabilização

Using and Entering Online Services Act	(PD – PA)		em casos de exploração sexual infantil, quando de boa-fé denunciassem casos suspeitos.
H.R.6713 (2008) / H.R.1166 (2009) - E-fencing Enforcement Act	Robert Scott (PD – WA)	31/07/2008 2ª vez 25/02/2009	Pretendia modificar o código criminal dos EUA para obrigar plataformas digitais a reter e fornecer informações sobre vendedores de produtos roubados online.
H.R. 4059 - Online Age Verification and Child Safety Act	Bart Stupak (PD – WI)	06/11/2009	Trata de proibição de exibição de conteúdo adulto para crianças e adolescentes e comercialização de produtos não indicados para menores de 18 anos.
S.3804 - Combating Online Infringement and Counterfeits Act	Patrick Leahy (PD – VT)	20/09/2010	Prevê responsabilização de plataformas digitais que ignorem ação judicial para bloqueio de atividade ilegal na web.
S.913 (2011) / S.418 (2013) / S.2404 (2015) - Do-Not-Track Online Act	John D. Rockefeller (PD – WV) Richard Blumenthal (PD – NY)	09/05/2011 2ª vez 28/02/2013 3ª vez 15/12/2015	Previa a criação de normas de regulação para a coleta e tratamento de dados dos usuários de serviços digitais.
S.968 - Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property - PROTECT IP Act	Patrick Leahy (PD – VT)	12/05/2011	Aumenta a responsabilização de plataformas digitais por associação a atividades ilegais de sites estrangeiros.
H. R.1895 (2011) / S.1700 / H.R.3481 (2013) / S.1563/ H.R.2734 (2015) / S.2932 / H.R.5930 (2018) - Do-Not-Track Kids Act	Edward J. Markey (PD – MA) Joe Barton (PR – TX)	13/05/2011 2ª vez 14/11/2013 3ª vez 11/06/2015 4ª vez 23/05/2018	Criava exigências e proibições para plataformas digitais coletarem e tratarem dados de crianças e menores entre 12 e 17 anos.
H.R.3261 - Stop Online Piracy Act	Lamar Smith (PR – TX)	26/10/2011	Exige que serviços online bloqueiem sites e plataformas digitais que façam distribuição de material pirateado. O bloqueio deve ser feito a partir de uma ordem judicial.
S.2029 / H.R.3782 - Online Protection and Enforcement of Digital Trade Act – OPEN Act	Ron Wyden (PD – OR) Darrell E. Issa (PR – OH)	17/12/2011 18/01/2012	O projeto prevê responsabilização de plataformas digitais de publicidade e transações financeiras que se associam a sites que infringem Lei de direitos autorais e marcas protegidas.

H. R. 6377 - Mobile Device Privacy Act	Edward J. Markey (PD – MA)	12/09/2012	Obrigada plataformas digitais a comunicar os usuários sobre instalação de software de monitoramento de atividades digitais.
H.R. 491 - Global Online Freedom Act	Christopher Smith (PR – NJ)	04/02/2013	Obrigava empresas estadunidenses a manter a liberdade de expressão na internet, mesmo em países onde houvesse restrições impostas por governos totalitários.
H.R.983 / H.R.656 - Online Communications and Geolocation Protection Act	Zoe Lofgren (PD – CA)	06/03/2013 2ª vez 02/02/2015	Proibia governo e plataformas digitais de divulgar dados de geolocalização de indivíduos sem mandado judicial.
H. R. 1312 / S. 639 - Geolocational Privacy and Surveillance Act	Jason Chaffetz (PR – CA) Wyden Ron (PD – KS)	21/03/2013	Proibia governo e plataformas digitais de divulgar dados de geolocalização de indivíduos sem mandado judicial.
H.R.2645 - Forbidding Advertisement Through Child Exploitation - FACE Act	John J. Duncan, Jr. (PR – TN)	10/07/2013	Proíbe plataformas de mídias sociais de utilizarem imagens de menores com intenções comerciais.
H. R. 4711 / S. 2378 (2014) / H.R.1053 / S.547 (2015) / H.R.4543 / S.2187 (2017) - Commercial Privacy Bill of Rights Act	Albio Sires (PD – NJ) Robert Menendez (PD – NY)	21/05/2014 2ª vez 24/02/2015 3ª vez 04/12/2017	Estabelecia parâmetros de tratamento de dados de usuários em atividades comerciais da plataforma digital.
S.2871 (2014) / S.512 / H.R.1174 (2015) - Law Enforcement Access to Data Stored Abroad Act	Orrin Hatch (PR – PA) Tom Marino (PR – PA)	18/09/2014 2ªvez 12/02/2015 27/02/2015	Criava uma série de exigências para que as plataformas digitais fornecessem informações de investigações a agências de investigação.
H.R.5586 (2016) / H.R.3520 (2017) / H.R.2687 (2019) / H.R.5744 (2021) - Customer Non-Discrimination Act	Bonnie Watson Coleman (PD – NJ)	24/06/2016 2ª vez 27/07/2017 3ª vez 10/05/2019 4ª vez 26/10/2021	Institui a obrigatoriedade de tratamento igualitário, inclusive em ambiente digital, para pessoa de qualquer sexo, identidade de gênero ou orientação sexual.
H.R.3175 (2017) / H.R.4978 (2019) / H.R.6027 – Online Privacy Act	Keith Ellison (PD – MN) Anna G. Eshoo (PD – CA)	11/07/2017 2ª vez 05/11/2019 3ª vez	Estabelece normas para coleta, tratamento e compartilhamento de dados de usuários das redes sociais. Cria uma Agência de Privacidade de Dados.

		18/11/2021	
S.2639 / H. R. 5815 - Customer Online Notification for Stopping Edge-provider Network Transgressions - CONSENT Act	Edward J. Markey (PD – MA) Michael E. Capuano (PD – MA)	10/04/2018 15/05/2018	Exige que plataformas digitais informem consumidores sobre o uso de dados pessoais, consigam consentimento para venda e compartilhamento destes dados, desenvolver práticas de segurança das informações e notificar usuários de vazamento dos dados.
S.2728 (2018) / S.189 (2019) / S.1667 (2021) - Social Media Privacy Protection and Consumer Rights	Amy Klobuchar (PD – MN)	23/04/2018 2ª vez 17/01/2019 3ª vez 18/05/2021	Exige que as plataformas digitais informem o usuário, antes de aderir ao serviço, que seus dados serão utilizados pela empresa e por terceiros.
S. 3127 (2018) / S.2125 / H.R.4536 (2019) - Bot Disclosure and Accountability Act	Dianne Feinstein (PD – CA) Elissa Slotkin (PD – MI)	25/06/2018 2ª vez 16/07/2019 26/09/2019	Exige que as plataformas de mídias sociais identifiquem e informem publicamente a ocorrência de *bots*, que simulam a interação humana, além de criar estratégias para remover este tipo de ação.
H.R.6917 (2018) / H.R.8013 (2022) - Remove Explicit Material Offensive to Victims Expeditiously Act - REMOVE Act	Luke Messer (PR – IN) Ann Kuster (PD – NH)	26/09/2018 2ª vez 09/06/2022	Requer que a FTC crie um site que torne possível o preenchimento de um formulário para que usuários de internet verifiquem se há imagens suas de cunho sexual postadas na internet e peçam aos provedores a remoção do conteúdo.
S.3744 (2018) / S. 2961 (2019) / S.919 (2021) - Data CARE Act	Brian Schatz (PD – HI)	12/12/2018 2ª vez 22/12/2019 3ª vez 23/03/2021	Impõe várias obrigações a plataformas digitais que tratam dados pessoais que podem ser relacionados ao usuário.
H.R.7363 (2018) / H.R.492 (2019) - Biased Algorithm Deterrence Act	Louie Gohmert (PR – TX)	20/12/2018 2ª vez 11/01/2019	Considera as plataformas digitais responsáveis por conteúdo de terceiros quando utilizam atividade algorítmica para oferecer *posts* fora da ordem cronológica, restringe ou bloqueia conteúdo de acordo com normas próprias de seleção e não a Lei.
S.806 - Own Your Own Data Act	John Kennedy (PR – LA)	14/03/2019	Exige que plataformas de mídias sociais permitam a portabilidade dos dados de usuários e quaisquer análises feitas a partir destas informações; e, garantir que os usuários forneçam consentimento para o tratamento dos dados.

S.1951 (2019) / H. R. 8512 (2020) / H.R.7120 (2022) - Designing Accounting Safeguards to Help Broaden Oversight and Regulations on Data – DASHBOARD Act	Mark R. Warner (PD – IN) Bill Foster (PD – IL)	25/06/2019 2ª vez 02/10/2020 3ª vez 17/03/2022	Exige que os operadores de dados comerciais divulguem quais são os dados coletados, o uso e valor dessas informações. Os operadores devem fornecer uma maneira de exclusão dos dados.
S.1914 - Ending Support for Internet Censorship Act	Josh Hawley (PR – MO)	19/06/2019	Proíbe plataformas de mídias sociais de fazer a moderação de conteúdo politicamente tendencioso.
H. R.4027 (2019) / H.R.7808 (2020) / H. R. 8612 (2022) - Stop the Censorship Act	Paul A. Gosar (PR – AZ)	25/07/2019 2ª vez 29/07/2020 3ª vez 29/07/2022	Limita a imunidade das plataformas de mídias sociais pela triagem ou bloqueio de conteúdo ofensivo na plataforma, considerado legalmente aceito.
S.2314 - Social Media Addiction Reduction Technology Act - SMART Act	Josh Hawley (PR – MO)	30/07/2019	Exigem que as plataformas digitais criem formas de mitigação de vício em seus serviços.
H.R.4232 (2019) / H.R.1107 (2021) - Protecting Local Authority and Neighborhoods Act - PLAN Act	Ed Case (PD – HI)	06/09/2019 2ª vez 18/02/2021	Limita a imunidade das plataformas digitais, especialmente quando permitem que conteúdo de terceiros possibilite a aplicação de golpes imobiliários.
H.R.4782 - National Commission on Online Platforms and Homeland Security Act	Bennie G. Thompson (PD – MS)	22/10/2019	Cria uma comissão que vai analisar como as plataformas digitais vem sendo usadas para promover ou apoiar campanhas de violência direcionada (terrorismo), assim como influência de estados estrangeiros nos EUA. A comissão deve exigir respostas das plataformas digitais e elaborar recomendações de mitigação do problema.
H.R.4813 - Keep Big Tech Out of Finance Act	Jesus G. "Chuy" Garcia (PD – IL)	23/10/2019	Proíbe empresas de tecnologia, como plataformas digitais de mídias sociais de oferecerem serviços de instituição financeira, ter como sócio uma instituição financeira ou oferecer moedas digitais.
H.R.5209 - Raising the Bar Act	Max Rose (PD – NY)	21/11/2019	Cria um programa que convoca as plataformas digitais a participarem de estudo para moderação de conteúdo na identificação de material terrorista.
H.R.5376 / S. 3007 (2019) / H.R.1198 / S. 365 (2021) - Eliminate Network Distribution	Anthony Gonzalez (PR – OH)	10/12/2019 2ª vez 22/02/2021	Obrigada as plataformas digitais a conservarem por 90 a 180 dias o conteúdo de exploração sexual

of Child Exploitation Act - END Child Exploitation Act	Marsha Blackburn (PR – MS)	23/02/2021	infantil denunciado pela CyberTipline do NCMEC.
H.R.5398 (2019) / H.R.1546 (2021) - Combating Online Wildlife Trafficking Act	Earl L. "Buddy" Carter (PR – GA)	11/12/2019 2ª vez 03/03/2021	Cria uma força-tarefa que investiga o tráfico online de animais e faz recomendações às plataformas para mitigação do problema.
S.3398 / H.R.8454 (2020) / S.3538 / H.R.6544 (2022) - Eliminating Abusive and Rampant Neglect of Interactive Technologies Act - EARN IT Act	Lindsey Graham (PR – SC) Sylvia R. Garcia (PD – TX)	05/03/2020 30/09/2020 2ª vez 31/01/2022 01/02/2022	Limita a imunidade das plataformas digitais em caso de propagação de material exploração sexual infantil e substitui o termo pornografia para abuso sexual infantil.
S.3455 / H.R.6896 (2020) / S.1143 / H.R.2566 (2021) - No TikTok on Government Devices Act	Josh Hawley (PR – MO) Ken Buck (PR – NY)	12/03/2020 15/05/2020 2ª vez 15/04/2021	Requer a remoção do TikTok de qualquer serviço online das agências de inteligência estadunidenses.
H. R 6586 / H.R.4653 - Social Media Accountability and Account Verification Act	Adam Kinzinger (PR – IL)	21/04/2020 2ª vez 22/07/2021	Obriga as plataformas a removerem contas falsas de suas redes sociais.
H. R. 6587 (2020) / H.R.4654 (2021) - Social Media Fraud Mitigation Act	Adam Kinzinger (PR – IL)	21/04/2020 2ª vez 22/07/2021	Criminaliza a abertura de contas falsas em plataformas de mídias sociais.
S.3629 / H.R.6752 (2020) / H.R.807 / S.223 (2021) - Invest in Child Safety Act	Ron Wyden (PD – OR) Anna G. Eshoo (PD – CA)	06/05/2020 08/05/2020 2ª vez 04/02/2021	Exigia a guarda de material de indivíduos investigados por exploração sexual infantil.
S.3983 / H.R.8596 - Limiting Section 230 Immunity to Good Samaritans Act	Josh Hawley (PR – MO) Ted Budd (PR – CN)	17/06/2020 16/10/2020 2ª vez 12/01/2021	Requer que os provedores de serviços online, inclusive plataformas de mídias sociais, mantenham atualizados seus termos de serviço, para evitar a responsabilização pela postagem de conteúdo de terceiros.
S.4062 - Stopping Big Tech's Censorship Act	Kelly Loeffler (PR – GA)	22/06/2020	Modifica as exigências que os provedores de serviços online têm para imunidade por conteúdo de terceiros.
H.R.7300 - Defund Executive Orders that Suppress Free Speech Act	Norma J. Torres (PD – CA)	22/06/2020	Proíbe o uso da verba federal 13925, que faz uma petição à FCC para fazer normas regulatórias para clarificar a responsabilidade civil das plataformas digitais por

			moderação de conteúdo de terceiros.
S.4066 (2020) / S.797 (2021) - Platform Accountability and Consumer Transparency Act - PACT Act	Brian Schatz (PD – HI)	24/06//2020 2ª vez 17/03/2021	Exige que as plataformas digitais mantenham seus termos de serviço atualizado, prevendo política de conteúdo permitido e prevejam forma de denúncia por conteúdo ilegal.
S.4534 - Online Freedom and Viewpoint Diversity Act	Roger F. Wicker (PR – MS)	08/09/2020	Limita a imunidade de uma plataforma digital que faz triagem e bloqueio de material ofensivo, revisa a aplicabilidade da responsabilidade civil por moderação de conteúdo inapropriado.
S.4632 - Online Content Policy Modernization Act	Lindsey Graham (PR – SC)	21/09/2020	Cria o Conselho de Reivindicações de Direitos Autorais, para decidir disputas de direitos autorais de menor valor. Limita a imunidade de um provedor ou usuário para triagem e bloqueio de material ofensivo na plataforma do serviço.
H.R.8323 - Bianca's Law	Anthony Brindisi (PD – NY)	21/09/2020	Exige que as empresas de mídia social estabeleçam um escritório para identificar e lidar representações gráficas de ferimentos ou morte que violem os padrões de moderação de conteúdo.
S.4756 / H.R.8515 (2020) / S.2335 (2021) - Don't Push My Buttons Act	John Kennedy (PR – LA) Paul A. Gosar (PR – AZ)	29/09/2020 02/10/2020 2ª vez 13/07/2021	Remove a imunidade de plataformas digitais que coletam informações sobre preferências ou crenças de um usuário e utilizam uma função automatizada para fornecer conteúdo com base nessas informações.
S.4758 (2020) / S.27 (2021) - See Something, Say Something Online Act	Joe Manchin III (PD – WV)	29/09/2020 2ª vez 22/01/2021	Exigia que plataformas digitais detivessem qualquer tipo de transmissão suspeita de dados, com relação a possível ameaça terrorista.
H.R.8517 (2020) / H.R.3827 (2021) - Protect Speech Act	Jim Jordan (PR – OH)	02/10/2020 2ª vez 11/06/2021	Modifica os termos de imunidade de responsabilidade civil de plataformas digitais que fazem moderação de conteúdo, com base em suas crenças. Pode haver reconsideração em caso de termos de serviço publicado, que ofereçam detalhamento sobre conteúdo permitido e se a plataforma agiu de boa-fé.

H.R.8636 (2020) / H.R.2154 / S.3029 (2021) - Protecting Americans from Dangerous Algorithms Act	Tom Malinowski (PD – NJ) Ben Ray Lujan (PD – NM)	20/10/2020 2ª vez 23/03/2021	Remove a imunidade de empresa de mídia social com mais de 10 milhões de usuários que utiliza algoritmo para recomendar conteúdo que envolva: interferência nos direitos civis ou atos de terrorismo internacional.
S.4828 - Stop Suppressing Speech Act	Kelly Loeffler (PR – GA)	21/10/2020	Elimina a imunidade de plataformas digitais que restringem conteúdo que seja censurável e aplica essa imunidade apenas na moderação de conteúdo ilegal, violento ou terrorista.
H.R.8719 (2020) / H.R.285 (2021) - Curbing Abuse and Saving Expression in Technology Act - CASE-IT Act	W. Gregory Steube (PR – FL)	30/10/2020 2ª vez 12/01/2021	Remove por um ano a proteção de ser tratado como publicador de informações quando a plataforma facilitar conteúdo online ilegal; contato de explorador com menores; ou, conteúdo indecente, obsceno ou prejudicial a menores.
S.4965 (2020) / H.R.7799 (2022) - Public Servant Protection Act	Tom Cotton (PR – AR) J. French Hill (PR – AR)	03/12/2020 2ª vez 17/05/2022	Permite que funcionários do governo exijam que pessoas e provedores de serviços de plataformas digitais removam certas formas de suas informações pessoais da Internet.
H.R.8896 (2020) / H.R.874 (2021) - Abandoning Online Censorship Act - AOC Act	Louie Gohmert (PR – TX)	08/12/2020 2ª vez 05/02/2021	Revoga a Seção 230 da Lei de Comunicações de 1934, que protege um serviço de computador interativo da responsabilidade pela triagem ou bloqueio de conteúdo censurável.
S.4975 (2020) / S.427 / H.R.5803 (2021) - Promoting Responsibility Over Moderation in the Social-media Environment - PROMISE Act	Mike Lee (PR – AZ) Tom Rice (PR – SC)	08/12/2020 2ª vez 24/02/2021 01/11/2021	Exige que as plataformas digitais estabeleçam e divulguem políticas de moderação de conteúdo, incluindo as categorias que não são permitidas, o processo de moderação e como o provedor faz a notificação de material moderado.
H.R.8922 - Break Up Big Tech Act	Tulsi Gabbard (PD – HI)	09/12/2020	Remove a imunidade de um provedor de serviço de computador interativo que se envolve com a venda e exibição de publicidade personalizada sem o consentimento do usuário.
S.5012 - Holding Sexual Predators and Online Enablers Accountable Act	Kelly Loeffler (PR – GA)	11/12/2020	Estabelece nova infração penal por possuir, gerenciar ou operar uma plataforma digital que promova ou facilite a hospedagem ou o tráfico de materiais que

			envolvam exploração sexual infantil.
S.5020 (2020) / S.2972 (2021) - A bill to repeal section 230 of the Communications Act of 1934	Lindsey Graham (PR – SC)	15/12/2020 2ª vez 07/10/2021	Pede a revogação da seção 230 da Lei de Comunicação de 1934 por ação de moderação de conteúdo das plataformas digitais.
H.R.9043 - Online Terrorism Prevention Act	Josh Gottheimer (PD – NJ)	21/12/2020	Exige que as empresas de mídia social estabeleçam um escritório para identificar e remover conteúdo violento ou extremista associado ou distribuído por uma organização terrorista. O projeto prevê a execução pela FTC, pelos procuradores gerais dos estados e pelo FBI.
S.5085 - A bill to amend the Internal Revenue Code of 1986 to increase the additional 2020 recovery rebates, to repeal section 230 of the Communications Act of 1934, and for other purposes.	Mitch McConnell (PR – AL)	29/12/2020	Revoga a imunidade de responsabilidade de uma plataforma digital para triagem e bloqueio de conteúdo ofensivo e aborda a administração de eleições federais.
H.R.83 - Protecting Constitutional Rights from Online Platform Censorship Act	Scott DesJarlais (PR - IA)	04/01/2021	Elimina a imunidade de responsabilidade civil de uma plataforma digital por restringir material ofensivo e proíbe uma plataforma de Internet de tomar medidas para restringir o material de um usuário protegido pela Constituição ou Lei federal, estadual ou local.
S.299 / H.R.3421 - Safeguarding Against Fraud, Exploitation, Threats, Extremism, and Consumer Harms Act - SAFE TECH Act	Mark R. Warner (PD – IN) A. Donald McEachin (PD – VA)	08/02/2021 20/05/2021	Elimina a imunidade de responsabilidade civil quando o usuário ou a plataforma digital aceitar o pagamento para disponibilizar um discurso; criar ou financiar (no todo ou em parte) o discurso.
H.R.1543 - No Social Media Accounts for Terrorists or State Sponsors of Terrorism Act	Andy Barr (PR – KY)	03/03/2021	Proíbe o acesso a certas plataformas de mídia social por indivíduos designados como terroristas ou altos funcionários de um governo que patrocina terrorismo
H.R.2000 - Stop Shielding Culpable Platforms Act	Jim Banks (PR – IN)	18/03/2021	Modifica as disposições sobre responsabilidade de uma plataforma digital por conteúdo divulgado de outro provedor de informação.
S.1384 / H.R.7613 - 21st Century Foundation for the Right to Express and Engage in	Bill Hagerty (PR – TN)	27/04/2021 28/04/2021	Retira a imunidade de responsabilidade civil para plataformas digitais ou usuários

Speech Act - 21st Century FREE Speech Act	Marjorie Taylor Greene (PR – GA)		que realizam certos atos afirmativos, como barrar usuários do serviço ou restringir o acesso ou a disponibilidade de material.
H.R.3057 - Anti-CCP Espionage via Social Media Act - ACES Act	Lisa C. McClain (PR – MI)	07/05/2021	Proíbe certas transações de qualquer pessoa sujeita à jurisdição dos EUA com a ByteDance, controladora chinesa do TikTok.
H.R.3184 - Civil Rights Modernization Act	Yvette D. Clarke (PD – NY)	13/05/2021	Especifica que a proteção de responsabilidade de uma plataforma digital sobre conteúdo de terceiros não se aplica a determinados anúncios direcionados a usuários que fazem parte de uma classe protegida ou têm um estado protegido.
H.R.3451 - Social Media Disclosure and Transparency of Advertisements Act - Social Media DATA Act	Lori Trahan (PD – MA)	20/05/2021	Exige que sites voltados para o consumidor e app com muitos usuários mantenham bibliotecas de anúncios e as disponibilizem para pesquisadores acadêmicos e para a FTC.
S.1896 / H.R.3611 – Algorithmic Justice and Online Platform Transparency Act	Edward J. Markey (PD – MA) Doris O. Matsui (PD – AZ)	27/05/2021 28/05/2021	Estabelece requisitos para plataformas digitais que retêm ou promovem conteúdo por meio de algoritmos e processos computacionais relacionados que usam informações pessoais.
S. 2031 - Promoting Rights and Online Speech Protections to Ensure Every Consumer is Heard Act - PRO-SPEECH Act	Roger F. Wicker (PR – MS)	10/06/2021	Proíbe as plataformas digitais de restringir o acesso ao conteúdo e se envolver em conduta discriminatória ou anticompetitiva de seleção de conteúdo, app ou serviços legalmente protegidos. Proíbe ainda discriminação por motivos de afiliação racial, sexual, religiosa, étnica ou política.
S. 2228 - Disincentivizing Internet Service Censorship of Online Users and Restrictions on Speech and Expression Act - DISCOURSE Act	Marco Rubio (PR – FL)	24/06/2021	Remove as proteções de responsabilidade de plataformas digitais com grande participação de mercado quando promove ou suprime um ponto de vista por meio de sua moderação de conteúdo, inclusive afetando a receita de um criador de conteúdo; usa algoritmos para direcionar e ampliar conteúdo; ou solicita, financia, modifica conteúdo.
H.R.4240 - User Data Protection Act	David Schweikert	29/06/2021	Estabelece requisitos para sites e outras plataformas digitais que

	(PR – CA)		coletam e armazenam informações sobre seus usuários. Proíbe coleta sem consentimento, restrição a acesso, em caso de recusa de coleta, usar pixel oculto para coleta ou compartilhar dados com terceiros.
S.2338 - Preserving Political Speech Online Act	Steve Daines (PR – CA)	14/07/2021	Exige que as plataformas digitais deem as mesmas condições de anúncio publicitário para conteúdo eleitoral pago.
S.2448 - Health Misinformation Act	Amy Klobuchar (PD – MN)	22/07/2021	Limita a proteção de responsabilidade das plataformas digitais quando relacionada ao conteúdo de terceiros que promove desinformação sobre saúde durante uma emergência de saúde pública declarada.
S.2500 - PRESERVE Online Speech Act	Marco Rubio (PR – FL)	28/07/2021	Exige que as plataformas digitais emitam divulgação pública relacionada a uma solicitação ou recomendação de uma entidade governamental para que o serviço modere o conteúdo em sua plataforma.
S.2725 (2021) / H.R.7819 (2022) - Accountability for Online Firearms Marketplaces Act	Richard Blumenthal (PD – NY) Jason Crow (PD – WI)	13/09/2021 18/05/2022	Remove a proteção de responsabilidade de plataforma digital que recebe por conteúdo fornecido por terceiros, se o provedor operar um mercado de armas de fogo online.
H.R.5449 / S.2917 - Federal Big Tech Tort Act	Lance Gooden (PR – TX) Josh Hawley (PR – MO)	30/09/2021	Cria um direito privado de ação contra uma empresa de mídia social quando um indivíduo com menos de 16 anos sofre lesão corporal ou danos à saúde mental que é atribuível, no todo ou em parte, ao uso do site de uma empresa de mídia social, aplicativo online ou aplicativo móvel.
H.R.5596 - Justice Against Malicious Algorithms Act	Frank Pallone, Jr. (PD – NJ)	15/10/2021	Limita a proteção de responsabilidade federal que se aplica a uma plataforma digital para reivindicações relacionadas ao conteúdo fornecido por terceiros que causem danos físicos ou emocionais.
S.3608 - Nudging Users to Drive Good Experiences on Social Media Act - Social Media NUDGE Act	Amy Klobuchar (PD – MN)	09/02/2022	Exige que a FTC identifique intervenções de plataforma independentes de conteúdo para reduzir os danos da amplificação algorítmica e do vício em mídia social em plataformas cobertas e

			para outros fins. Prevê cooperação em estudos e implementação de normas regulatórias a partir das pesquisas.
H.R.6755 - Cooperation Among Police, Tech, and Users to Resist Exploitation Act - CAPTURE Act	Gus M. Bilirakis (PR – FL)	18/02/2022	Instrui o Governo Federal a estudar e relatar ao Congresso levantamento feito em conjunto com empresas de mídia social e forças de segurança sobre conteúdo ilegal na rede.
H.R.6796 - Digital Services Oversight and Safety Act	Lori Trahan (PD – MA)	18/02/2022	Estabelece o Bureau of Digital Services Oversight and Safety dentro da FTC para supervisionar a moderação de conteúdo por plataformas digitais.
H.R.6918 - No Publicity for Terrorists Act	Madison Cawthorn (PR – NC)	03/03/2022	Obriga plataformas de mídias sociais a derrubar, em 24 horas, contas de indivíduos sabidamente envolvidos com atividade terrorista.
S.4201 / H.R 7858 - Digital Platform Commission Act	Michael Bennet (PD – CO) Peter Welch (PD – MA)	12/05/2022 19/05/2022	Estabelecer um novo órgão federal para fornecer supervisão e regulamentação razoáveis de plataformas digitais.
H.R.8041 - China Social Media Reciprocity Act	Brian J. Mast (PR – MI)	13/06/2022	Fornece autoridade para proibir a prestação de serviços por plataformas de mídia social a indivíduos e entidades na Lista de Cidadãos Especialmente Designados e certos funcionários e outros indivíduos e entidades da República Popular da China.
H.R.8152 - American Data Privacy and Protection Act	Frank Jr. Pallone (PD – NJ)	21/06/2022	Propõe normas para o tratamento de dados de cidadãos estadunidenses e impõe obrigações às plataformas digitais.
H.R.8409 - Countering Foreign Malign Influence Act	Sean Patrick Maloney (PD – NY)	18/07/2022	Faz modificações relacionadas ao Centro de Dados de Mídia Social e Análise de Ameaças com o objetivo de melhorar ações cooperativas para detectar e combater operações de influência estrangeira nos EUA.
H.R.8752 - Protecting Speech from Government Interference Act	James Comer (PR – TN)	30/08/2022	Proíbe funcionários de agências executivas ou que estão no serviço competitivo de censurar o discurso de outras pessoas enquanto atuam em funções oficiais, incluindo ordenar ou defender a

			remoção do discurso legal de uma plataforma.
H.R.8772 - Block the Tok Act	Dusty Johnson (PR – SD)	06/09/2022	Proíbe o aplicativo de mídia social TikTok de acessar dados de usuários estadunidenses na China e exige que a FCC investigue se o TikTok se envolveu em práticas injustas ou enganosas.
H.R.8946 - Online Dating Safety Act	David G. Valadao (PR – CA)	21/09/2022	Exige que as plataformas digitais que promovem encontros sejam obrigadas a fornecer notificações de fraudes e verificação de identidade de usuários.
S.4963 - Combating Cartels on Social Media Act	Kyrsten Sinema (PD – AZ)	27/09/2022	Exige que o DHS relate e implemente uma estratégia para combater o uso de mídias sociais por organizações criminosas transnacionais para recrutar indivíduos nos Estados Unidos para apoiar atividades ilícitas no País ou em suas fronteiras.
H.R.9448 - Free Speech Defense Act	Andrew S. Clyde (PR – GA)	07/12/2022	Proíbe a criação de normas de regulação federal das plataformas de mídias sociais que instituam a remoção de contas ou conteúdo; que preveja a rotulação de falso ou verdadeiro para informações; e, que obrigue compartilhamento de dados pessoais de cidadãos com o governo.
H.R.9508 / S.5245 - Averting the National Threat of Internet Surveillance, Oppressive Censorship, and Influence - ANTI-SOCIAL CCP Act	Mike Gallagher (PR – WI) Marco Rubio (PR – FL)	13/12/2022	Proíbe o aplicativo de mídia social TikTok de fazer negociações em território estadunidense.

Fonte: Elaborado pela autora

Além dos projetos de Lei que foram discutidos no período de levantamento, entre 2006 e 2022, esta tese analisa ainda quatro Leis que foram aprovadas ou revisadas no mesmo período, que estão detalhadas no Quadro 14.

Quadro 14 – Leis que regulam plataformas digitais que entraram em vigor nos EUA entre 2006 e 2022

MECANISMO LEGAL	AUTORES	DATAS	RESUMO DA PROPOSTA
Broadband Data Improvement Act - Public Law No. 110-385, 2008	Daniel K. Inouye (PD – MI)	10/10/2008	Requer que a FCC compile uma lista de áreas geográficas que não são atendidas por nenhum provedor de capacidade avançada

			de telecomunicações para que os serviços sejam disponibilizados aos cidadãos estadunidenses.
Providing Resources, Officers, and Technology to Eradicate Cyber Threats to Our Children Act - PROTECT Our Children Act - Public Law No: 110-401, 2008	Joseph R. Biden Jr. (PD – DE)	13/10/2008	Exige que o Departamento de Justiça desenvolva e implemente um Sistema Nacional de Prevenção e Interdição da Exploração Infantil, com uma Força-Tarefa para Crimes na Internet Contra Crianças.
Children's Online Privacy Protection Act – COPPA Rule, 2013	FTC	17/01/2013	A Comissão altera o Proteção da privacidade on-line das crianças na COPPA, consistente com os requisitos de proteção da privacidade on-line das crianças pelas mudanças tecnológicas registradas desde o ano 2000.
Allow States and Victims to Fight Online Sex Trafficking Act - Public Law No. 115-164, 2018	Ann Wagner (PR – MO)	11/04/2018	A Lei reconhece que a seção 230 da Lei de Comunicações de 1934 não se destinava a fornecer proteção legal a sites que promovem e facilitam ilegalmente a prostituição e a sites que facilitam aos traficantes a publicidade da venda de atos sexuais ilegais com vítimas de tráfico sexual.

Fonte: Elaboradora pela autora.

A análise dos instrumentos regulatórios dos EUA vai seguir a mesma dinâmica proposta para a legislação brasileira, com a seguinte dinâmica: as Leis serão analisadas na integralidade, já os projetos de Lei serão agrupados nas temáticas que estão propostas nesta tese que considera as normas referentes à liberdade de expressão, privacidade e segurança do usuário. Sendo consideradas como normas referentes à liberdade de expressão aquelas ligadas à moderação de conteúdo, as de privacidade que tratam da utilização de dados e segurança as que estiverem ligadas a combate ao crime em ambiente digital ou hábitos adictos. Por tratar-se de número extenso de projetos de Lei, os instrumentos serão resumidos. A análise inicia-se pelas Leis.

5.3.2.1 Broadband Data Improvement Act - Public Law Nº 110-385, 2008

Apresentada em maio de 2007, a proposta do senador Daniel Inouye, tratava da melhoria na oferta de serviços de banda larga nos EUA. O objetivo era melhorar a

qualidade técnica e garantir que mesmo áreas remotas do país tivessem acesso a sinal de boa qualidade. A fiscalização ficou a cargo da FCC, que deveria conduzir estudos de locais ainda não atendidos pelos serviços. Outro propósito da Lei era impedir a interferência dos provedores de internet na oferta de conteúdo, principalmente relacionado aos serviços de *streaming* audiovisual, que estavam em desenvolvimento. O que vinha ocorrendo eram ações de redução de velocidade de transmissão que interferia no recebimento do conteúdo pelos usuários.

Apesar desta Lei tratar, principalmente, de sinal de internet, ela entra no escopo desta tese porque a este instrumento foi anexado o projeto Protecting Children in the 21st Century Act (S. 1965), apresentado, em janeiro de 2007, pelo senador Ted Stevens. O projeto teve pequenas alterações no texto e foi reintroduzido em agosto do mesmo ano (S. 49). A proposta trazia uma série de exigências a órgãos ligados ao governo, mudança em políticas educacionais referentes à prevenção de divulgação de pornografia infantil na web em bibliotecas e escolas. Com relação às plataformas digitais previa a responsabilização em caso de divulgação de vídeos contendo pornografia infantil. O texto propunha triplicar multas para plataformas digitais que falhassem em denunciar casos de pornografia infantil e não colocassem avisos sobre presença de conteúdo sexual explícito em postagens divulgadas em seus ambientes online.

A proposta proibia ainda a comercialização de dados sabidamente pertencentes a crianças. O texto reconhecia como predadores sexuais indivíduos que abordassem crianças e adolescentes em salas de bate papo online e redes sociais. Além disso, impunha uma série de obrigações às plataformas quanto à atividade de menores em seus ambientes digitais, tais como: identificação, consentimento dos pais para utilização dos serviços e aplicação de política anti-ciberbullying em seus ambientes digitais. Toda a fiscalização do cumprimento das normas ficou a cargo da FTC e os procuradores-gerais dos estados foram habilitados também a processar as empresas em caso de lesão coletiva.

5.3.2.2 Providing Resources, Officers, and Technology to Eradicate Cyber Threats to Our Children Act - PROTECT Our Children Act - Public Law Nº 110-401, 2008

A legislatura de 2007-2008 foi profícua em projetos de Lei de combate à exploração sexual infantil na internet. Além do projeto de Lei Protecting Children in the

21st Century, que foi aprovado e promulgado em 2008, anexado à Lei Nº 110-385 (10/10/2008). Vários projetos com a mesma temática foram apresentados tanto na câmara como no senado, tratando do combate à pornografia infantil na web. Algumas propostas foram anexadas e aprovadas como legislação, caso da Lei Nº 110-401.

Em fevereiro de 2007, foi apresentado conjuntamente na câmara e senado, o projeto Securing Adolescents From Exploitation-Online Act – SAFE Act (S. 519 / H. R. 876), do deputado Steve Chabot e do senador John McCain. O projeto previa a emenda ao código criminal dos EUA para obrigar as plataformas digitais a reportarem casos suspeitos de exploração sexual infantil. Na denúncia, as plataformas seriam obrigadas a fornecer identificação dos ofensores, incluindo endereço de e-mail, site ou local de divulgação das imagens, hora em que as imagens foram carregadas, informações geográficas para localização do ofensor e preservação das provas.

As plataformas só estariam imunes de responsabilização em caso de colaborarem com a ação de combate à pedofilia. Exigia ainda a divulgação de relatórios sobre investigações desta natureza ao procurador-geral dos EUA. Estes projetos estavam relacionados à proposta Protecting Children from Pornography and Internet Exploitation Act - PROTECT Our Children Act (S. 3344), introduzida pelo senador Tom Coburn, que também previa exigir das plataformas digitais a obrigação de relatar casos suspeitos de violação à Lei de pornografia infantil.

Estes projetos foram anexados à proposta Providing Resources, Officers, and Technology to Eradicate Cyber Threats to Our Children Act, que também utilizou o título reduzido de PROTECT Our Children Act (S. 1738), do senador Joseph Biden, apresentado em junho de 2007, que foi introduzido na câmara, no mês seguinte, pela deputada Debbie Wasserman Schultz (H. R. 3845). O objetivo da proposta era a criação de uma política pública de combate à pornografia infantil na internet. Para isso, foi estabelecida uma estratégia nacional de combate a crimes contra crianças na internet, com a instalação da National Internet Crimes Against Children Data System, que foi designada para investigação e prevenção de conduta ilegal dentro desta temática. A Lei criou dotação orçamentária para a implementação de tais políticas.

Quando solicitados por agências de investigação estrangeiras dados sobre comercialização de pornografia infantil, as plataformas digitais foram obrigadas a comunicar as autoridades estadunidenses, se falharem neste aviso devem ser multadas. Quando não-intencional a multa estabelecida é de US$ 150 mil, em casos intencionais o valor dobra. De acordo com o texto, o instrumento legal não pode ser

utilizado para monitoramento de atividade de usuários, por ofensa à privacidade dos cidadãos estadunidenses, porém, quando solicitadas por investigações as plataformas são obrigadas a colaborar.

Denúncias feitas pelo CyberTipline do National Center of Missing and Exploited Children (NCMEC) devem ser comunicados às forças policiais, porém, os dados só poderão ser compartilhados com envolvidos diretamente nas investigações e as provas devem ser preservadas pelas plataformas, por até 90 dias após a notificação. O material deve ter acesso mitigado entre os funcionários das empresas de tecnologia, com destruição de material apenas a partir da requisição de agência federal de investigação.

5.3.2.3 Children's Online Privacy Protection Act – COPPA Rule, 2013

A Children Online Privacy Protection, mais conhecida como COPPA, foi aprovada em 1998. A COPPA exigiu que os operadores de sites ou serviços online direcionados a crianças menores de 13 anos notificassem aos pais e obtivessem consentimento deles antes de coletar, usar ou divulgar dados pessoais. A Lei também obrigava as plataformas a manter seguras as informações que coletassem de crianças. O uso comercial da internet nos EUA estava completando quase uma década, porém, ainda não havia uma real dimensão do poder da rede.

A COPPA já passou por duas revisões, uma em 2000, que fica fora do nosso escopo de análise e a outra em 2013, por isso foi selecionada. A segunda revisão teve seu processo de alteração iniciado em 2010 e demorou três anos para ser concluída. Em 2021 teve início mais uma discussão no Senado para nova atualização da COPPA (S. 1628), porém não chegou a ser votada. A última proposta de revisão previa maior controle dos pais sobre a coleta e tratamento de dados de menores em sites ou serviços direcionados a crianças que integram serviços externos, como plug-ins ou redes de publicidade.

Em 2013, a atualização da COPPA ampliou o escopo de efeito da Lei, além de sites, serviços online e aplicativos voltados especificamente a crianças, foram incluídas plataformas que oferecem os mesmos serviços a audiência em geral, mas que a plataforma tem conhecimento que podem ser acessadas por menores de 13 anos. Foi proibida ainda a coleta de dados de crianças em plataformas digitais por serviços de terceiros utilizando *plug-ins,* sem consentimento parental. Serviços de

cobrança terceirizados, assim como plataformas de publicidade que coletam dados de visitantes também foram incluídos na norma.

Além de informações como nome, sobrenome, endereço, número de telefone, informações de contato online ou captura de tela de computador, foram incluídos dados de geolocalização, fotos, vídeos e áudios que correspondam a uma criança. A atualização incluiu ainda serviços de identificadores persistentes, como *cookies*, que rastreiam a atividade online de menores. Nesta última regra há uma ressalva para empresas que utilizam *cookies* apenas para suas operações internas de manutenção do serviço.

Foi criada nesta revisão a figura do Safe Harbor, que contou com o auxílio das seguintes instituições: Aristotle International, Inc., a Children's Advertising Review Unit of the Council of Better Business Bureaus, ESRB Privacy Online, PRIVO e TRUSTe. Plataformas digitais que aderissem aos programas de auto conformidade destas instituições estariam livres de investigações da Comissão Federal de Comércio. Os programas de auto conformidade compreendem diretrizes e procedimentos disciplinares para determinadas atividades das plataformas digitais, que oferecem serviços para menores de 13 anos, já que a norma só previa proteção a crianças de 0 a 12 anos completos.

Foram oferecidos às empresas processos simplificados para conseguir consentimento dos pais para tratamento de dados infantis. As empresas precisaram assumir compromisso sobre a segurança no armazenamento destes dados. Foram estabelecidas normas para a retenção e para a exclusão destas informações. Foi delegado à Comissão Federal de Comércio a fiscalização das diretrizes e procedimentos disciplinares referente às instituições de Safe Harbor.

O consentimento parental na coleta e tratamento de dados pessoais de crianças foi modificado, permitindo a utilização de formulários online; vídeo conferência; identificação emitida pelo governo; sistemas de pagamento alternativos, como uso de cartão de débito ou cobrança eletrônica. Para empresas que utilizam os dados de crianças internamente foi aceito o consentimento parental via e-mail. No caso de compartilhamento de informações, as empresas só foram autorizadas a dividir dados com prestadores de serviço ou parceiros que apresentassem condições de manter confidencialidade e segurança das informações. As empresas que aderiram ao programa de Safe Harbor têm suas normas autorregulatórias auditadas por terceiros. As normas entraram em vigor em 2013.

Whiting (2023) observa que a Comissão Federal do Comércio falhou em fiscalizar o cumprimento da COPPA até o momento, com poucas punições por violações e baixa emissão de multas, com valores irrisórios para empresas de tecnologia. Além disso, as normas de Safe Harbor protegem demasiadamente as empresas que aderem ao programa.

A título de exemplificação, Wang (2022) enumerou 39 reclamações analisadas pela Comissão Federal de Comércio e Advogados Gerais de Estado em março de 2022 a respeito de irregularidades referentes à COPPA. Deste total, 22 se referiam a coleta de dados de menores sem consentimento dos pais. Pelo menos 12 reclamações se referiam a compartilhamento de informações de crianças com plataformas de marketing direcionado. Em fevereiro de 2022, o Youtube recebeu uma multa de US$ 170 milhões por violações da COPPA, o valor corresponde a cerca de 1,1% do faturamento da empresa.

5.3.2.4 Allow States and Victims to Fight Online Sex Trafficking Act – SESTA /FOSTA – Law 115–164, 2018

A Lei aprovada foi introduzida na Câmara em 2017 pela deputada Ann Wagner, o projeto foi chamado de Allow States and Victims to Fight Online Sex Trafficking Act (H. R. 1865), que ficou conhecido como FOSTA. A proposta avançou na câmara e no senado, onde havia sido apresentado o projeto de Lei Stop Enabling Sex Traffickers Act – SESTA (S. 1693). Por tratarem do mesmo tema, os dois projetos foram fundidos e a Lei foi aprovada e promulgada em 2018, sob o codinome FOSTA/SESTA.

A Lei emenda a Communication Act de 1934, e altera a seção 230 da Communication Decency Act de 1996, tornando serviços interativos de computador e seus usuários responsáveis por conteúdo que incentiva e promove prostituição, facilita o tráfico sexual ou anuncia a venda de atos sexuais de vítimas de exploração. As plataformas de mídias sociais foram reconhecidas pela corte estadunidense como parte dos serviços interativos de computador, que devem moderar o conteúdo com teor sexual, no sentido de prevenir e combater a promoção à prostituição e tráfico sexual.

Como pondera DeLacey (2022), o projeto de Lei nasceu a partir de uma investigação sobre o serviço dos sites Backpage.com e Craigslist.com, que permitiam o anúncio de serviços, inclusive adultos. Os sites foram acusados de facilitar o tráfico sexual, incluindo menores. O Backpage enfrentou vários processos, porém, juízes

consideraram a plataforma inocente, com base na imunidade prevista pela seção 230 da Communication Decency Act, de 1996, que impedia a responsabilização de intermediários pelo conteúdo de terceiros. Uma investigação de 18 meses provou que o Backpage estaria consciente da facilitação do tráfico sexual e este foi o estopim para a criação do projeto de Lei.

A Lei prevê multa e pena de prisão de até 10 anos para quem promove a prostituição ou divulga material de exploração sexual de vítimas de tráfico humano em território estadunidense ou estrangeiro. A pena pode ser agravada, com até 25 anos de reclusão, se o criminoso é o explorador de cinco ou mais pessoas; ou ainda, se está diretamente ligado à exploração sexual e tráfico de pessoas.

McCracken, Howell e Thomson (2018) pontuam que grandes companhias de redes sociais têm seus instrumentos de moderação e conseguem dar tratamento ao problema, porém, vão moderar conteúdo com base estrita para evitarem ações judiciais, prejudicando liberdade de expressão e banindo qualquer conteúdo sexual de suas plataformas. Pequenos serviços interativos de computador não teriam estrutura e condições de manter uma moderação mais restritiva, o que os colocaria em risco de ação judicial. Com isso, a Lei pode prejudicar a inovação tecnológica.

A Lei prevê que as vítimas de exploração ou tráfico sexual têm direito a advogado e recebimento de indenização. Os acusados de facilitação ou incentivo à prostituição poderão se defender das acusações, caso provem que o meretrício era legalizado no território onde a denúncia foi feita e que não houve ação de tráfico de pessoa ou exploração de vítimas. O crime, segundo a Lei, reside na participação do indivíduo em um empreendimento que auxilia, apoia ou facilita a prostituição. Neste caso, os procuradores-gerais dos estados, com base na Lei, podem mover ações civis públicas quando identificarem condutas que prejudicam os moradores de sua localidade.

Para DeLacey (2022) o objetivo do instrumento legal era combater o tráfico e a exploração sexual, porém, a Lei atingiu os trabalhadores do sexo como um todo. Além disso, interferiu na liberdade de expressão, por conta da responsabilidade que plataformas digitais podem enfrentar, mediante publicação de conteúdo sexual, mesmo sem restrição legal. A Lei não foi capaz ainda de tratar o problema para o qual foi criada, já que o tráfico e a exploração sexual persistem, principalmente em

plataformas estrangeiras e na *dark web*[45], que torna a investigação de crimes ainda mais difícil.

No prazo de 3 anos da promulgação da Lei, um relatório deveria ser emitido pelo procurador-geral dos EUA com detalhamento dos processos julgados com base na Lei, categorizando por tipo de denúncia, qualidade do réu, valor de pedido de indenizações, ações procedentes ou não. Para Citron e Jurecic (2022) a moderação de conteúdo relacionado ao sexo, por atacado, silenciou comunidades vulneráveis e trabalhadores do setor. O problema da exploração e tráfico sexual continuam, o que prova o fracasso da FOSTA/SESTA. Este resultado tornou a mudança da seção 230 da CDA uma tarefa ainda mais difícil para os legisladores, deixando as plataformas digitais livres de responsabilizações que elas poderiam enfrentar.

5.3.2.5 Projetos de Lei referentes à liberdade de expressão

O primeiro projeto de Lei que tratava única e exclusivamente sobre a liberdade de expressão na internet foi apresentado em fevereiro de 2013, pelo deputado Christopher Smith (PR – NJ), sob o título Global Online Freedom Act (H. R. 491). O escopo do projeto tratava da liberdade de expressão não só no território estadunidense, mas trazia como obrigação às empresas nacionais a manutenção deste direito inclusive no exterior, em países que tentassem exercer censura sobre a rede. O texto do projeto reconhecia a importância da internet na manutenção do direito fundamental de liberdade de expressão e o avanço de países totalitários sobre esta ferramenta.

A proposta exigia das plataformas digitais a inclusão em relatórios anuais a diligência na preservação de direitos humanos; políticas relativas ao tratamento de dados pessoais; e, possíveis restrições em serviços de busca, assim como, compartilhamento de conteúdo. Estes relatórios deveriam trazer o nome do país, onde a liberdade de expressão estaria sendo restringida, com identificação da agência governamental que estivesse exercendo a censura. Haveria imunidade para empresas que tivessem certificação da Global Network Iniciative, tratada na seção 3.4 desta tese (p. 77). O projeto de Lei previa, ainda, a proibição de exportação de

[45] "Dark web" ou "deep web" é o termo utilizado para servidores de rede disponíveis na internet utilizados somente por meio de ferramentas, com configurações e autorizações específicas, prezando o anonimato dos usuários. Por isso mesmo, é utilizada para acesso em países totalitários que monitoram a atividade dos cidadãos e para atividades ilegais.

equipamentos e tecnologia para países em que houvesse restrição à internet. Também exigia das empresas a publicação de suas políticas referentes à liberdade de expressão, com auditoria externa sobre o cumprimento das normas por parte de funcionários e parceiros.

Em fevereiro de 2016, a deputada Bonnie Watson Coleman (PD – NJ), introduziu o projeto de Lei Customer Non-Discrimination Act (H.R.5586), A proposta propunha uma emenda ao código civil estadunidense de 1964, em sua seção 201, para inserir o tratamento igualitário em locais público para qualquer sexo, identidade de gênero ou orientação sexual, incluindo não apenas ambientes físicos, mas também digitais. O projeto foi reapresentado em 2017 (H.R.3520), novamente em 2019 (H.R.2687) e por último, em 2021 (H.R.5744). O texto do projeto foi praticamente mantido em todas as versões, sem mudança de objetivos.

Com exceção dos projetos anteriores, a partir de 2017, quase a totalidade das normas propostas previa a modificação da seção 230 da Communications Act of 1934, ou até mesmo a sua exclusão e construção de um novo dispositivo legal. A seção 230 dá imunidade aos provedores de serviços online pelo conteúdo de terceiros, porque segundo a norma, as plataformas digitais são consideradas apenas conduítes de material. Como intermediárias, as plataformas digitais não teriam responsabilidade civil pela publicação de terceiros.

A maioria dos projetos, no entanto, tratam de modificações na seção 230. O que tem movido os legisladores, principalmente, é a ação algorítmica de seleção de conteúdo, que aumenta ou reduz distribuição de material, bloqueia e até exclui contas e usuários, de acordo com o que a plataforma considera censurável, mesmo que o conteúdo esteja protegido pela Lei. Há ainda a manutenção de conteúdo reconhecidamente ilegal, que as plataformas se negam a retirar.

Em dezembro de 2018, o deputado Louie Gohmert (PR – TX) propôs o projeto Biased Algorithm Deterrence Act (H. R. 7363), que foi reapresentado no ano seguinte (H. R. 492), prevendo responsabilização como editoras para plataformas digitais que utilizassem algoritmos para moderação de conteúdo. A norma previa a responsabilização civil de plataformas de mídias sociais que utilizassem qualquer ação de atraso, potencialização ou bloqueio de conteúdo, por meio de algoritmos. O instrumento legal previa a transformação da plataforma digital em editora do material e não apenas intermediária, como um canal de divulgação.

Em junho de 2019, o senador Josh Hawley (PR – MO) trouxe à discussão o projeto Ending Support for Internet Censorship Act (S. 1914) que previa a proibição de moderação de conteúdo político pelas plataformas digitais de forma tendenciosa, não podendo fazer modificações ou ações algorítmicas contra partidos, candidatos ou pontos de vista. O projeto previa a criação de um certificado de imunidade, emitido pela FTC, com duração de dois anos, como forma de reconhecimento de que a plataforma digital seria apenas intermediária de conteúdo, desde que provasse não ter moderado conteúdo político no período. A emissão e renovação do certificado deveriam ser feitas no prazo de seis meses, com análise de todos os dados fornecidos pela plataforma digital. As sanções para os infratores deveriam ser aplicadas pela FTC.

O projeto de Lei Stop the Censorship Act (H.R.7808 / H.R.4027 / H.R.8612) do deputado Paul A. Gosar (PR – AZ) foi introduzido três vezes na Câmara. A primeira em julho de 2019, a segunda vez em julho de 2020 e, por fim, em julho de 2022. Na primeira versão a norma propunha tornar as plataformas responsáveis quando estas fizessem exclusão ou redução de distribuição de material legalmente aceitável, apenas por considerar o assunto censurável. Na segunda versão foi introduzida a possibilidade de imunidade apenas quando a plataforma excluísse material que incitasse a violência ou terrorismo. Na última versão, o texto voltou a ser redigido como no original.

O projeto de Paul A. Gosar (PR – AZ) estava relacionado à proposta Stop Suppressing Speech Act (S. 4828), da senadora Kelly Loeffler (PR – GA), apresentada em 2020. A autora acrescentou a possibilidade de que os usuários deveriam ter à disposição um mecanismo no qual escolhessem com quais assuntos não gostariam de ter contato, ao invés da plataforma fazer esta seleção. Com isso, a plataforma estaria imune de punições apenas em caso de moderação de conteúdo ilegal e não de material considerado por ela censurável. Naquele mesmo ano, a senadora já havia introduzido o projeto Stopping Big Tech's Censorship Act (S.4062), que tratava da mesma questão, prevendo multa às plataformas digitais que fizessem moderação de conteúdo em desacordo com a Primeira Emenda da Constituição dos EUA, que institui a base da liberdade de expressão estadunidense.

Ainda em 2020, o senador Josh Hawley (PR – MO) também propôs a retirada de imunidade das plataformas digitais em caso de moderação de conteúdo de forma discriminatória ou tendenciosa, com o projeto Limiting Section 230 Immunity to Good

Samaritans Act (S. 3983). O projeto foi introduzido na Câmara (H.R.8596) pelo deputado Ted Budd (PR – NC) e reintroduzido na legislatura seguinte pelo mesmo deputado (H.R.277). Resumidamente, o instrumento legal propunha obrigar as plataformas digitais a manterem termos de serviço, com detalhamento sobre moderação de conteúdo, vinculando-se a um dever contratual de boa-fé com seus usuários. O projeto previa que a aplicação seletiva de suas normas de serviço tornaria a plataforma sujeita a multas, por descumprimento de cláusula contratual.

Prabhu (2020) indica que há discordâncias entre os legisladores sobre movimentos para imposição de padrões de moderação de conteúdo para as redes sociais digitais. Neste sentido, poderia haver requisitos legais para a imposição de moderação de desinformação, com a instituição de um padrão federal para tratamento da questão, prevendo a identificação de autenticidade de usuários, ações seletivas de criptografia, para investigação de possíveis ameaças, e, monitoramento de entrada de atores estrangeiros em plataformas estadunidenses. A partir da identificação da influência de atores estrangeiros em campanhas de desinformação na internet poderiam ser implementadas ações efetivas de punição destas influências.

A deputada Norma J. Torres (PD – CA) introduziu, em junho de 2020, o projeto Defund Executive Orders that Suppress Free Speech Act (H.R.7300), que previa a proibição de utilização de verba federal para cumprimento da Ordem Executiva 13.925, emitida pelo então presidente Donald Trump, para prevenção à censura online. A Ordem Executiva impunha à FCC a criação de normas regulatórias sobre a moderação de conteúdo feita pelas plataformas digitais. De acordo com o texto da Ordem Executiva, a moderação de conteúdo não poderia ser feita de forma discriminatória quanto a orientação política, religiosa, racial ou sexual.

No mesmo mês, o senador Brian Schatz (PD – HI) introduziu o projeto Platform Accountability and Consumer Transparency Act – PACT Act (S.4066) para obrigar plataformas digitais a publicarem termos de uso aceitáveis, sistema de denúncia para remoção de publicações e relatórios bianuais de moderação. O projeto não chegou a evoluir na legislatura 116 e acabou introduzido novamente em março de 2021 (S. 797). O texto teve pequenas alterações com detalhamento sobre a compensação ao produtor de conteúdo, que tivesse seu material removido e com isso perdesse monetização. Já previsto no projeto original, a remoção de conteúdo deveria ser acompanhada de notificação ao usuário, com possibilidade de defesa. Quanto à plataforma, além das multas aplicadas pela FTC, por moderação fora do padrão,

também poderia ser considerada responsável civilmente caso fosse notificada judicialmente de conteúdo ilegal postado em sua rede e se negasse a removê-lo.

Com a mesma lógica de necessidade de que os termos de uso fossem mais claros e transparentes aos usuários foram apresentados os projetos Protect Speech Act (H.R.8517 / H.R.3827), do deputado Jim Jordan (PR – OH); e Promoting Responsibility Over Moderation In the Social-media Environment - PROMISE Act (S.4975 / S.427), do senador Mike Lee (PR – AZ), com apoio do deputado Tom Rice (PR – SC) (H.R.5803). Ambos foram apresentados consecutivamente em 2020 e 2021, tratando da responsabilização das plataformas digitais pela moderação de material, que não deveria ter sido removido, porque seria conteúdo legalmente aceito e apenas era considerado censurável pela plataforma digital.

Alguns projetos propunham a eliminação da seção 230 e uma nova discussão de parâmetros de responsabilização das plataformas digitais pelo conteúdo propagado em seus ambientes online. Este foi o caso dos projetos Abandoning Online Censorship Act – AOC Act (H.R.8896 / H.R.874), do deputado Louie Gouhmert e no senado A bill to repeal section 230 of the Communication Act of 1934 (S.5020 / S.2972), da senadora Lindsey Graham (PR – SC). Ambos foram introduzidos duas vezes, em 2020 e 2021. Em 2020, o projeto de Graham (S.5020), foi relacionado ao projeto de Lei do senador Mitch McConnell (PR – AL), A bill to amend the Internal Revenue Code of 1986 to increase the additional 2020 recovery rebates, to repeal section 230 of the Communications Act of 1934, and for other purposes (S.5085), que basicamente, com relação às plataformas digitais, tratava das mesmas questões com relação à responsabilização por conteúdo de terceiros.

Graham destacou no texto de sua proposta de Lei (S.5020 / S.2972) que a seção 230, criada em 1996, teve a intenção de proteger empresas incipientes de mídia, que estavam começando seus negócios e precisavam de segurança jurídica para atuar, sem ter de responder por erros de terceiros. Com o aumento das companhias, porém, esta proteção já não se justificaria, porque as empresas se transformaram em oligopólios, teriam dominado a seara pública e o discurso da sociedade.

Apresentado, em abril de 2021, conjuntamente pelo senador Bill Hagerty (PR – TN) e pela deputada Marjorie Taylor Greene (PR – GA), em suas respectivas casas legislativas, o projeto 21st Century Foundation for the Right to Express and Engage in Speech Act, ou apenas 21st Century FREE Speech Act (S.1384 / H.R.7613) também

tratou da abolição da seção 230, criando um novo artigo (232), que traria em sua redação a exigência de acesso não-discriminatório e transparência na oferta dos serviços, com abertura das práticas de moderação de conteúdo. A proposta trazia a imunidade em caso de conteúdo de terceiros, porém, previa a responsabilização para as práticas discriminatórias de moderação. De acordo com o texto, linhas telefônicas não seriam desligadas de acordo com a opinião política de quem estava na ligação, desta forma, o mesmo tratamento deveria ser dado aos perfis de redes sociais.

Em 2021 também foi introduzido o projeto Protecting Constitutional Rights from Online Platform Censorship Act, (H.R.83) do deputado Scott DesJarias. Os projetos trazem basicamente as mesmas referências, de termos de serviço com linguagem clara, objetiva e possibilidade de o usuário buscar indenização quando se sentir lesado no processo de moderação de conteúdo da plataforma digital. Apresentado pelo senador Edward J. Markey (PD – MA) e pela deputada Doris O. Matsui (PD – AZ), em maio de 2021, o projeto Algorithmic Justice and Online Platform Transparency Act (S.1896 / H.R.3611) fez uma série de exigências às plataformas digitais que utilizam algoritmos para moderação, impulsionamento ou direcionamento de conteúdo. A proposta previa a ação não-discriminatória por uso de algoritmos, além do cuidado das plataformas com a possibilidade de influência do cidadão em seu direito de voto. A proposta previa a contribuição de denúncias de usuários e a investigação de irregularidades por meio de agências federais, por ação discriminatória algorítmica.

Proposto pelo senador Roger F. Wicker (PR – MS), em junho de 2021, o projeto de Lei Promoting Rights and Online Speech Protections to Ensure Every Consumer is Heard Act, foi apelidado de PRO-SPEECH Act (S.2031). O PRO-SPEECH Act proíbe as plataformas digitais de bloquear acesso a conteúdo considerado legal, que não interfere em sua funcionalidade. O projeto de Lei reafirma que as plataformas não poderiam interferir no conteúdo de terceiros, considerado legal. As plataformas ficariam impedidas de ter qualquer comportamento discriminatório com base em raça, religião, filiação política ou etnia, por meio de ação algorítmica. O projeto propõe ainda a divulgação de um relatório, que demonstre as políticas e práticas comerciais de *app store*, de serviço de busca, de armazenagem, SEO e de mídia social, que oportunize ao consumidor informações suficientes para aquisição de produto ou serviço divulgado na plataforma digital.

Keller (2021) pontua que infelizmente a ação algorítmica das plataformas digitais de moderação de conteúdo pode excluir conteúdo legal. A IA pode, por exemplo, retirar do ar um documentário sobre crimes de guerra na Síria, sob a ótica de combate a conteúdo terrorista na rede, como já ocorreu com vídeos no Youtube. O projeto de Lei teria de fazer uma ponderação do que seria melhor para a sociedade, a aplicação deste tipo de filtro, com possibilidade de revisão de ação, ou a inação das plataformas, com a propagação de todo tipo de conteúdo sem utilização alguma de ação algorítmica para moderação. Caso projetos de Lei como este fossem aprovados, o risco seria de que ações de moderação algorítmica fossem retiradas pelas plataformas para evitar penalidades.

Especificando um pouco mais um mecanismo legal, a senadora Amy Klobuchar (PD – MN) propôs, em julho de 2021, o projeto de Lei Health Misinformation Act (S. 2448), que tratou apenas de informações de saúde em períodos de emergência sanitária. A pandemia de Covid-19 ainda estava vigente e a senadora propunha que as plataformas fossem responsabilizadas por propagação de desinformação de saúde, quando houvesse ação algorítmica de distribuição e impulsionamento de conteúdo. A manutenção da imunidade só seria reconhecida em caso de demonstração de distribuição de conteúdo de saúde por meios cronológicos e não algorítmicos.

O impulsionamento ou anúncio de conteúdo político foi tratado pelo Steve Daines (PR – CA), no projeto de Lei Preserving Political Speech Online Act (S.2338), de julho de 2021. A proposta previa que o tratamento dado a conteúdo publicitário eleitoral veiculados nas plataformas digitais deveria ter tratamento igualitário para os políticos anunciantes. Os anúncios políticos não poderiam ser censurados por questões ideológicas, além disso, todos os registros de publicidade política deveriam estar disponíveis ao público em até 24 horas após a contratação. A regulação da propaganda política digital ficaria a cargo da FTC.

O projeto de Lei Disincentivizing Internet Service Censorship of Online Users and Restrictions on Speech and Expression Act - DISCOURSE Act (S.2228), proposto pelo senador Marco Rubio (PR – FL), em junho de 2021, trouxe novamente a mesma temática: o uso de algoritmos para seleção, potencialização de alcance ou bloqueio de conteúdo tornaria as plataformas digitais responsáveis pelo conteúdo de terceiros. No mesmo ano, o senador ainda propôs o projeto PRESERVE Online Speech Act (S.2500), que exigia das plataformas digitais a transparência a respeito de pedidos de

agências do governo para moderação de conteúdo e remoção de perfis online. Com aplicação de multa para descumprimento da divulgação pública das informações.

Proposta semelhante fez o deputado James Comer (PR – TN), em agosto de 2022, com o projeto de Lei Protecting Speech from Government Interference Act (H. R. 8752). No caso deste projeto, a proibição seria de que qualquer funcionário federal promovesse ou apoiasse a censura de discurso nas redes sociais. Os servidores ficariam proibidos de fazer pedidos de remoção de conteúdo ou perfis nas plataformas digitais, com exceção apenas para casos de conduta ilegal. Na mesma linha, no encerramento do ano de 2022, o deputado Andrew S. Clyde (PR – GA) apresentou o projeto de Lei Free Speech Defense Act (H.R.9448) a partir da divulgação dos relatórios do Twitter e do Facebook, sobre a supressão de *posts* e perfis, a pedido do FBI e de outras agências federais, assim como do serviço de segurança dos EUA.

Em resumo, a proposta previa a proibição de que o governo federal de coagisse ou encorajasse mídias sociais a moderarem ou rotularem conteúdo de usuários; proibia financiamento federal para criação de conselhos de desinformação; proibia aceite de publicidade gratuita para funcionários do governo em redes sociais; e, exigia relatórios anuais de conformidade com a Lei (H.R.9448).

Conteúdo ligado à comercialização de armas de fogo, transações neste sentido na rede e instruções sobre como imprimir uma arma em uma impressora 3D tornariam a plataforma digital responsável pelos *posts* de terceiros. Esta era a proposta feita pelo senador Richard Blumenthal (PD – NY), Accountability for Online Firearms Marketplaces Act (S.2725), apresentada em setembro de 2021, que foi apoiada pelo deputado Jason Crow (PD – WI), em maio de 2022, na câmara (H.R.7819).

Para Webb e Martineau (2022) falta conhecimento técnico às congressistas na elaboração da Lei e ainda de membros do setor de TI para compor as equipes que supostamente fariam os estudos. Além disso, ambas não reconhecem a possibilidade de mudança do ecossistema de plataforma com a aprovação da Lei. A simples presença de uma agência reguladora não estaria habilitada para lidar com o dinamismo da matéria. Até porque a liberdade de expressão, defendida na 1ª Emenda da Constituição Americana, estará sempre nas mãos das plataformas em corte.

Gellis (2022) salienta que o problema referente ao enfrentamento à 1ª Emenda da Constituição Americana pode se dar neste momento pós-estudos. Porque os resultados das pesquisas provavelmente vão mostrar quais são os conteúdos mais disseminados na rede. Neste momento, o que seria algoritmo neutro ou agnóstico,

passa a ter temas de moderação. A Lei, nesta fase, passa a colidir com a 1ª Emenda, que é categórica em dizer que os congressistas não podem legislar sobre liberdade de expressão.

Para Mackenzie-Gray Scott (2023), a falta de transparência das redes sociais em seu processo de moderação de conteúdo tira o poder de decisão do usuário. Quanto maior for a transparência do ambiente, melhor será a interação do usuário. Porém, falta educação para o uso das tecnologias e mesmo detalhada, talvez a informação não possa ser acessada por falta de conhecimento técnico dos usuários. Por isso, ações educacionais deveriam estar previstas na Lei.

5.3.2.6 Projetos de Lei referentes à liberdade de expressão e segurança

A liberdade de expressão e segurança eram temas da proposta do senador Byron Dorgan intitulada Internet Freedom Preservation Act (S. 215), apresentada em janeiro de 2007, que foi posteriormente introduzida na Câmara, em fevereiro do ano seguinte, pelo deputado Edward J. Markey (PD – MA), (H. R. 5353). Inicialmente, o texto trazia a necessidade de que as plataformas digitais garantissem serviço com segurança de rede e possibilidade de controle parental para acesso a conteúdo. Quando foi apresentado na Câmara o projeto trouxe ainda a preocupação de que as plataformas digitais não utilizassem mecanismos discriminatório de acesso aos seus serviços, baseado em origem, propriedade ou localização. O texto detalhou que os usuários deveriam ter livre acesso para visualização, recebimento e distribuição de conteúdo.

Em setembro de 2020, o senador Roger F. Wicker (PR – MS) apresentou o projeto de Lei Online Freedom and Viewpoint Diversity Act (S.4534). De acordo com o texto, para se livrar da responsabilidade civil pela remoção de conteúdo de terceiros, a plataforma deveria agir de boa-fé e justificar a ação pela crença de que o material moderado fosse obsceno, lascivo, excessivamente violento, de assédio, promotor de automutilação, terrorismo ou conduta ilegal. O projeto de Lei passaria a considerar a plataforma digital como editora de conteúdo quando modificasse substancialmente conteúdo de terceiros.

Para Weissmann (2022) o problema com este tipo de projeto de Lei é a tentativa de mudança da seção 230 do Communications Decency Act de 1996, que dá aos serviços de computador interativos a responsabilidade pela moderação de conteúdo

com uma abertura bastante extensa de suas aplicações, com possibilidade de interferência em material que consideram violento, ameaçador, lascivo, entre outras classificações. No ano de 2021, o Facebook relatou a exclusão de 25 milhões de *post* que, segundo a plataforma, tinham conteúdo de exploração sexual infantil. Com certeza, alguns dos *posts*, se analisados de perto, foram excluídos de forma errônea e isso poderia gerar multas à empresa.

O deputado Anthony Brindisi (PD – NY) propôs, em setembro de 2020, que as plataformas digitais criassem escritórios para tratar de conteúdo de violência explícita postada em suas redes. O projeto de Lei Bianca´s Law (H.R.8323) obrigaria as plataformas a manterem um escritório que fosse dedicado à identificação e remoção deste tipo de conteúdo na rede. As normas das plataformas deveriam prever que a postagem deste tipo de conteúdo seria proibida, e seus funcionários treinados a identificar e remover tais postagens. A ação de moderação deste tipo deveria passar por auditorias regulares e os resultados deveriam ser divulgados em relatórios periódicos. Toda a fiscalização desta norma ficaria a cargo da FTC.

Esta Lei foi proposta depois da morte de Bianca Devins, em 2019. A jovem de 17 anos foi assassinada e imagens de seu corpo já sem vida foram postadas pelo assassino, Brandon Clark Cicero, em diversas plataformas de mídias sociais como Facebook, Instagram, Twitter, Snapchat, YouTube e Discord. A família de Bianca abriu uma petição na internet, em que informou que as imagens permaneciam online e muitas pessoas já haviam denunciado o caso, porém, as plataformas respondiam que os *posts* não seriam contrários às suas regras da comunidade. Na petição, a família pedia o fim da imunidade de plataformas digitais que promovem, disseminam ou solicitam conteúdo ilegal; que tivessem conhecimento de conteúdo em seus ambientes digitais que contrariam à Lei; e, que não removem conteúdo ilegal, mesmo depois de notificação[46].

Associado à Bianca´s Law (H.R.8323) estava a proposta do deputado Josh Gottheimer (PD – NJ), Online Terrorism Prevention Act (H.R.9043). O projeto de Lei previa a manutenção de um escritório para identificação e combate a conteúdo violento e extremista, associado a organizações terroristas na rede, era a imposição proposta pelo, no final de 2020. A ação deveria ser feita com treinamento de

---

46 DEVINS, Kimberlly. Bianca’s Law - Stop the spread of violent and graphic images on the internet! Charge Org. Disponível em: https://www.change.org/p/bianca-s-law-stop-the-spread-of-violent-and-graphic-images-on-the-internet Acessado em: 22/07/2023.

funcionários, autorias e relatórios externos periódicos, com remoção imediata de conteúdo notificado pela FTC.

Para o senador Mark R. Warner (PD – IN), o aceite de dinheiro para impulsionamento de discurso faria da plataforma uma coautora de conteúdo. Por isso, em fevereiro de 2021, ele propôs o projeto Safeguarding Against Fraud, Exploitation, Threats, Extremism, and Consumer Harms Act - SAFE TECH Act (S. 299). A proposta vai além, reconhecendo a responsabilidade das plataformas ainda quando falharem em retirar conteúdo à Lei de direitos civis; Lei antitruste; Leis de perseguição, assédio ou intimidação; direito internacional dos direitos humanos; e ações civis por homicídio culposo. Um exemplo usado pelo senador foi do *dating app* Grindr, que havia se negado a tomar providências em casos de perseguição ocorridas no serviço online.

Para o autor, a imunidade não poderia se aplicar a conteúdos pagos; não impediria ação de medidas cautelares; não prejudicaria a aplicação de Leis de direitos civis, de Leis de prevenção de exploração sexual e violência; e, nem ações por contribuição em casos de homicídio culposo. O projeto de Lei também foi apresentado na Câmara, no mês de maio do mesmo ano, pelo deputado A. Donald MacEachin (H.R.3421). O mesmo entendimento foi apresentado pela deputada Yvette D. Clarke (PD – NY) na apresentação do projeto Civil Rights Modernization Act (H.R.3184), que basicamente propõe as mesmas inferências da seção 230, de que não é possível admitir imunidade no caso de conteúdo pago, e reconhece a viabilidade de ações judiciais e medidas cautelares em casos de desrespeitos a direitos civis.

O deputado Jim Banks (PR – IN) reconheceu que as plataformas podem até não ser consideradas editoras de conteúdo, porém, propôs pelo projeto Stop Shielding Culpable Platforms Act (H. R. 2000) que elas fossem reconhecidas como distribuidoras das informações, em caso de conteúdo ilegal postado, e, em consequência desta ação, pudessem ser responsabilizadas pelo material propagado. A propositura da Lei foi feita logo após divulgação de uma reportagem do New York Times sobre a hospedagem de contas que distribuíam imagens de estupros e exploração sexual de menores na plataforma Pornhub.

Nesta mesma linha, o deputado Frank Palone Jr. propôs o projeto de Lei Justice Against Malicious Algorithms Act (H. R. 5596), que reconheceria a responsabilidade de plataformas que fizessem a moderação algorítmica de conteúdo, com potencial de causar danos físicos ou emocionais a seus usuários. De acordo com o texto, a

recomendação personalizada, feita por ação algorítmica, acabaria expondo pessoas mais propensas a dano, de acordo com conteúdo sensível a estes indivíduos.

Em fevereiro de 2022, a deputada Lori Trahan (PD – MA) propôs o Digital Services Oversight and Safety Act (H.R.6796). O projeto previa a criação de um serviço, dentro da FTC, responsável por fiscalização a ação de moderação de conteúdo das plataformas digitais. O órgão teria poderes investigatórios, no caso de propagação de conteúdo ilegal, assim como ação discriminatória de grupos dentro das plataformas de mídias sociais. Além disso, poderia conduzir também investigações sobre ações hackers dentro dos ambientes digitais. A proposta ainda criou parâmetros de divulgação de ação de moderação por meio de termos de uso e relatórios das atividades. O mecanismo previu a regulamentação de recomendações automatizadas de conteúdo aos usuários dessas grandes plataformas.

5.3.2.7 Projetos de Lei referentes à privacidade

O monitoramento dos usuários de plataformas digitais foi o tema da proposta do senador John D. Rockefeller (PD – WV), apresentada em maio de 2011, sob o título Do-Not-Track Online Act (S.913). O texto requeria da FTC a criação de normas regulatórias para a coleta de dados dos usuários. Segundo a proposta, se fazia necessário um regramento para tratamento de dados, estabelecendo uma forma simples e clara de quais informações seriam coletadas, com qual finalidade e abrindo espaço para que o indivíduo pudesse negar a ação. As plataformas digitais seriam responsabilizadas em caso de dar continuidade à atividade de coleta sem consentimento, com uma única exceção para quando o tratamento de dados fosse indispensável para a oferta do serviço. A fiscalização e implementação das regras ficaria a cargo da FTC.

A proposta não passou na legislatura 112, e foi novamente apresentada por Rockefeller na 113 (S.418), sem alteração de texto. Em dezembro de 2015, na legislatura 114, foi mais vez apresentada (S.2404), desta vez pelo senador Richard Blumenthal (PD – NY), com pequenas alterações no texto, como previsão de penalidade para discriminação de usuários que não quisessem ter seus dados coletados, com detalhamento de quais informações pessoais não poderiam ser compartilhadas como IP de máquina, e-mail, prevendo, ainda, multa de US$ 500 a

cada violação da norma, com possiblidade de a corte triplicar o valor por ação deliberada de irregularidade.

Quando ainda era deputado, Edward J. Markey (PD – MA) introduziu na câmara o projeto Do-Not-Track Kids Act (H.R.1895), em maio de 2011, propondo alteração da COPPA, detalhada no ponto 5.3.2.3 desta tese. O projeto de Lei de Markey, tinha nome semelhante ao de Rockefeller (S.913), porém, tinha outro objeto, propunha regulação específica sobre tratamento de dados de crianças e adolescentes. Segundo o texto, as plataformas digitais estavam proibidas de coletar dados infantis e de menores entre 12 e 17 anos, quando estivessem cientes da idade dos usuários. As informações não poderiam ser compartilhadas com terceiros e nem utilizadas para marketing direcionado. A coleta de informações de geolocalização também estava prevista na proibição.

A Lei citava ainda o desenvolvimento de uma norma, a Digital Marketing Bill of Rights for Teens, que traria parâmetros para a inserção de conteúdo comercial para menores. As normas previam ações que visassem o esclarecimento comercial a menores, evitando práticas enganosas e injustas. O mecanismo instituía ainda a possibilidade de que os dados coletados de menores pudessem ser facilmente apagados da rede. Com execução e fiscalização prevista para a FTC. O projeto não passou naquela legislatura 112 e foi apresentado mais três vezes. Uma vez em 2013, quando Markey já era senador (S.1700) e foi introduzida também na câmara pelo deputado Joe Barton (PR – TX) (H.R.3481). Em 2015, a proposta foi novamente apresentada pelos mesmos parlamentares em suas respectivas casas (S.1563 / H.R.2734). Mais uma vez, em 2018, a proposta foi reintroduzida também em ambas as casas, pelos mesmos legisladores (S.2932 / H.R.5930).

Em 2013 (S.1700 / H.R.3481), a proposta exigiu consentimento parental comprovável, para a utilização dos serviços pela criança, assim como, não utilização de informações pessoais destes usuários para direcionamento de conteúdo de marketing. Para clientes entre acima de 12 e menores de 18 anos, bastava a autorização do menor para a coleta dos dados. A proposta recebeu apoio, em 2014, por meio do projeto de Lei Commercial Privacy Bill of Rights Act (H.R.4711 / S.2378) apresentado pelo deputado Albio Sires (PD – NJ), e pelo senador Robert Menendez (PD – NY). Este segundo projeto tratava de regulação sobre segurança de dados em atividades comerciais. A proposta apresentou o que Markey havia citado em sua

primeira apresentação do projeto Do-Not-Track Kids Act (H.R.1895), que era a figura da Digital Marketing Bill of Rights for Teens, com os direitos comerciais de menores.

Em resumo, o projeto de Lei Commercial Privacy Bill of Rights Act (H.R.4711 / S.2378) previa que os usuários fossem notificados sobre as práticas de tratamento de dados pelas plataformas digitais; exigia o aviso em caso de mudanças destas regras; indicava a autorização prévia do usuário para coleta de dados, compartilhamento com terceiros e direcionamento de marketing; e, que fornecessem ao usuário a oportunidade de correção de dados equivocados. O instrumento legal estabelecia a possibilidade de celebração de contratos para utilização das informações coletadas e restringia o período em que as empresas pudessem armazenar os dados coletados. O aviso por vazamento de informações ficava condicionado ao possível prejuízo ao qual o usuário estaria exposto e à quantidade de clientes atingidos, sendo exigido apenas para mais de 10 mil usuários, com informações sensíveis, em banco de dados governamentais ou de funcionários estatais.

Em 2015, o projeto Do-Not-Track Kids (S.1563 / H.R.2734) recebeu mudanças mínimas, que não interferiram no objetivo do instrumento legal. Já a Commercial Privacy Bill of Rights Act (H.R.1053 / S.547) voltou a ser apresentada em ambas as casas legislativas pelos mesmos parlamentares sem alteração alguma. No ano de 2017, Sires e Menendez (H.R.4543 / S.2187) reapresentaram sua proposta, novamente sem alteração. Em 2018, a proposta de Markey e Barton (S.2932 / H.R. 5930) previu que o consentimento parental para tratamento de dados fosse exigido também para menores entre 12 e 17 anos. Mesma exigência feita pela proposta Data Security and Breach Notification Act (S. 1976), do senador John Rockfeller.

Focando mais nos serviços móveis de comunicação, o deputado Edward J. Markey (PD – MA) apresentou em setembro de 2012 a proposta Mobile Device Privacy Act (H R.6377). Mas mesmo focado nos aparelhos celulares, o projeto previa que além de operadoras de celular, serviços de internet também comunicassem seus usuários sobre a instalação de softwares que fizessem o monitoramento de atividades digitais dos usuários. Os usuários deveriam ter a possibilidade de bloqueio de coleta e transmissão de dados a qualquer momento. Segundo a proposta, a FTC e a FCC seriam obrigadas a editar normas a respeito do tema e fiscalizar o cumprimento delas pelas empresas de tecnologia.

A preocupação com a divulgação da localização dos usuários de equipamentos móveis de comunicação seguiu em 2013, com a apresentação de dois projetos de Lei,

no mês de março: Online Communications and Geolocation Protection Act (H. R. 983), pela deputada Zoe Lofgren (PD – CA); Geolocational Privacy and Surveillance Act – GPS Act (H. R. 1312 / S. 639), do deputado Jason Chaffetz (PR – CA); e, do senador Ron Wyden (PD – OR). Apesar da nomenclatura diferente, os projetos eram bastante semelhantes. Com o GPS Act (H. R. 1312 / S. 639) sendo um pouco mais abrangente. Em resumo, os projetos previam a alteração da Lei criminal estadunidense para exigir que as plataformas digitais fornecessem dados de geolocalização mediante mandado judicial.

As propostas proibiam agências governamentais de interceptarem localização de cidadãos, com exceção para vigilância estrangeira, com base na Foreign Intelligence Surveillance Act of 1978 (FISA); mediante autorização do indivíduo, ou responsável, a quem pertencesse a informação; em caso de dados de acesso público; e, quando necessário para atendimento de emergência para socorro do indivíduo, ou risco à vida. As plataformas digitais seriam proibidas de fazer esta divulgação sem ação judicial que a justificasse. As propostas também previam a reparação de dano ao usuário que tivesse seus dados divulgados.

Neste mesmo sentido, o senador Orrin G. Hatch apresentou o projeto de Lei Law Enforcement Access to Data Stored Abroad Act (S.2871), em setembro de 2014, que previa exigências aos órgãos governamentais que requisitassem dados às plataformas digitais. De acordo com o texto, apenas seriam possíveis de obter dados extraterritoriais de cidadãos estadunidenses. A informação poderia estar armazenada tanto nos EUA como fora dele. Não seria possível que o destinatário da mensagem fosse obrigado a divulgá-la à autoridade policial. Uma cópia do mandado judicial, para a obtenção das informações deveria ser enviado à plataforma digital, que seriam obrigadas a atender a requisição.

Os pedidos governamentais teriam de ser divulgados em relatórios anuais pelas plataformas com a informação de qual órgão partiram os pedidos de informação. A proposta não passou e foi novamente apresentada em fevereiro de 2015, desta vez não só pelo senador Hatch (S.512), mas também na câmara, pelo deputado Tom Marino (PR – PA) (H.R.1174).

A preocupação com a propriedade dos dados e como os usuários deveriam ser tratados pelas plataformas digitais foi detalhado na proposta de deputado Keith Ellison (PD – MN), sob o título Online Privacy Act (H.R.3175), que previa notificação sobre coleta, consentimento para a finalidade proposta, discriminação contra aqueles que

não aceitassem os termos de tratamento de dados. A proposta não evolui e foi apresentada em legislaturas subsequentes pela deputada Anna G. Eshoo (PD – CA), que acrescentou ao texto a figura de uma Agência de Privacidade de Dados. Além disso, a parlamentar detalhou como deveria ser todo o processo de coleta, segurança de dados, para que as informações poderiam ser utilizadas e como o usuário manteria sua vontade, em detrimento dos interesses comerciais das plataformas digitais (H.R.4978 / H.R.6027).

No ano de 2018, teve maior ênfase a tentativa de regulação do consentimento do usuário para utilização de seus dados pessoais pelas plataformas digitais. O projeto Customer Online Notification for Stopping Edge-provider Network Transgressions – CONSENT Act (S.2639 / H.R.5815) foi apresentado em abril, pelo senador Edward J. Markey (PD – MA), e, em maio, pelo deputado Michael E. Capuano (PD – MA). O projeto especificava a necessidade de as plataformas notificarem e obterem consentimento dos clientes para a coleta, tratamento e compartilhamento de dados; obter consentimento para usar, compartilhar ou vender informações pessoais dos clientes; desenvolvimento de práticas de segurança de dados; e notificação dos clientes em caso de violação de segurança. A fiscalização e sanções ficariam a cargo da FTC.

Nas três últimas legislaturas o deputado Brian Schatz (PD – HI) apresentou o projeto de Lei Data Care Act (S. 3744 / S. 2961 / S. 919). Da primeira vez que veio a público em 2018, à última em 2021, a proposta teve pouca alteração e basicamente tratou de regramento para coleta, tratamento, armazenamento e compartilhamento de dados de usuários das plataformas digitais. Foi feita uma diferenciação para dados não identificáveis, que não são possíveis de associação a uma pessoa física e dados sensíveis que vão desde o cartão de seguro social do cidadão à localização do usuário via georreferenciamento.

De acordo com o texto, as plataformas digitais teriam deveres de cuidado, lealdade e confidencialidade com as informações dos seus usuários. O acesso não-autorizado aos dados deveria contar com medidas de proteção, para evitar que aconteçam. As práticas de segurança deveriam ser auditadas regularmente. Os dados pessoais não poderiam ser utilizados para prejudicar o dono das informações. As plataformas ficariam proibidas de vender e compartilhar dados de usuários com terceiros, quando não houvesse previsão contratual para tal finalidade. Seria obrigatória a comunicação de qualquer vazamento de informações. Os procuradores-

gerais dos estados poderiam mover ações quando os moradores de suas regiões pudessem ser prejudicados. Além disso, a FTC seria responsável pela fiscalização e aplicação de sanções e multas em caso de irregularidades apontadas.

Muito semelhante ao Data Care, a senadora Amy Klobuchar (PD – MN) propôs, a partir de 2018, em três legislaturas consecutivas, a Social Media Privacy Protection and Consumer Rights Act (S. 2728 / S. 189 / S. 1667) que previa obrigações às plataformas digitais referentes a informações que deveriam ser fornecidas aos usuários antes da adesão aos serviços oferecidos. A proposta obrigaria as plataformas a criarem personalização de preferências de privacidade. Com isso, os usuários poderiam selecionar quais informações poderiam ser coletadas e tratadas, porém, a personalização de tratamento de dados poderia autorizar as empresas a bloquearem seus serviços no todo, ou em parte, em caso de inoperabilidade tecnológica devido às escolhas do usuário.

O projeto de Lei imporia às plataformas a obrigatoriedade de oferecer cópias dos dados coletados do usuário, em caso de serem requisitadas. As empresas teriam obrigação de comunicação, em 72 horas, em caso de vazamento das informações do usuário. Estas plataformas digitais poderiam ser fiscalizadas e punidas com base neste regulamento pela FTC. Além disso, os estados também poderiam mover ações civis públicas em caso de identificação de dano coletivo aos seus moradores.

Na mesma linha dos anteriores, o senador John Kennedy (PR – LA) propôs, em março de 2019, o projeto de Lei Own Your Own Data (S.806). A proposta acrescentava a previsão de que a qualquer momento, as plataformas digitais fossem obrigadas a dar direito de portabilidade dos dados pessoais dos usuários que os requisitassem. Para que a ação fosse facilitada, o projeto previa a instalação de um botão ou ícone, em que o usuário pudesse clicar e imediatamente ter a cópia de seus dados tratados. Ainda previa que o usuário precisaria consentir com a exploração de seus dados por meio de termos de serviço de fácil compreensão, com no máximo 500 palavras, que fossem publicados e pudessem ser lidos antes da adesão ao serviço.

Também em 2019, o senador Mark R. Warner (PD – IN) apresentou o projeto de Lei Designing Accounting Safeguards To Help Broaden Oversight and Regulations on Data (S.1951), que previa também o consentimento para tratamento de dados, porém, acrescentando que o usuário deveria ter acesso a um relatório claro, com o valor aferido pelas plataformas digitais com os dados coletados e com quem negociavam. De acordo com o texto, as normas regulatórias deveriam ser editadas

pela Comissão de Valores Mobiliários. A proposta previa ainda um botão de exclusão que o usuário pudesse utilizar para que suas informações fossem removidas. Em 2020 e 2022, a proposta foi apresentada na câmara pelo deputado Bill Foster (PD – IL) (H.R.8512 / H.R.7120), sem alteração substancial de texto.

Voltando um pouco no tempo, o projeto Don't Push My Buttons Act (S.4756), do senador John Kennedy (PR – LA), apresentado em setembro de 2020, trouxe novamente à discussão a necessidade de que as plataformas digitais detivessem consentimento de usuários para tratamento de dados e fossem impedidas de direcionamento de conteúdo, a não ser que apresentassem autorização para esta finalidade. O projeto teve apoio do deputado Paul A. Gosar (PR – AZ), que o apresentou no mês seguinte na câmara (H.R.8515). Como não evoluiu naquela legislatura, foi novamente introduzido por Kennedy, em 2021 (S.2335).

A utilização dos dados dos usuários para direcionamento de publicidade tornaria as plataformas digitais responsáveis pelo conteúdo divulgado. Esta era a proposta da deputada Tulsi Gabbard (PD – HI), intutilada Break Up Big Tech Act (H.R.8922), apresentada em dezembro de 2020. Já a proposta da deputada Lori Traham, apresentada em maio de 2021, previa acesso de dados de anúncios a pesquisadores acadêmicos, assim como à FTC. O projeto Social Media Disclosure And Transparency of Advertisements Act – Social Media DATA Act (H.R.3451) trazia a especificação de um grupo de trabalho que deveria trazer determinações de quais seriam os acessos possíveis a dados pelos pesquisadores acadêmicos. As plataformas seriam obrigadas a manter bibliotecas de anúncios, com informações essenciais como conteúdo do anúncio, descrição de público-alvo e número de visualizações.

A privacidade dos servidores públicos estadunidenses teria maior valor do que dos cidadãos comuns. Esta foi a proposta apresentada, pelo senador Tom Cotton (PR – AR), em dezembro de 2020, sob o título Public Servant Protection Act (S.4965). De acordo com o texto, seria considerado crime revelar em mídias sociais dados sobre funcionários públicos, como nome e endereço, com intuito de causar dano a este indivíduo. Funcionários públicos poderiam exigir das empresas de mídias sociais que removessem suas informações da rede. A proposta foi detalhada em maio de 2022, pelo deputado J. French Hill (PR – AR) (H.R.7799), com a previsão de que a comunicação para retirada dos dados deveria ser feita por escrito e que as empresas

teriam 48 horas para executar a ordem, sob pena de pagamento de multa pela negativa na ação.

Muito próxima à LGPD (Lei Nº 13.7096, 2018) brasileira e ao RGPD europeu a proposta American Data Privacy and Protection Act (H.R.8152), apresentada em junho de 2022 pelo deputado Frank Jr. Pallone (PD – NJ) trouxe vários parâmetros para o tratamento de dados dos cidadãos estadunidenses. O regramento proposto instituía a obrigatoriedade de redução de utilização de dados pelas plataformas digitais, deveres de lealdade entre as empresas e seus usuários, no compartilhamento de dados com terceiros, apresentação obrigatória de consentimento para utilização das informações pessoais e a confecção de infraestruturas digitais que primassem pela privacidade do usuário. No âmbito comercial, o instrumento legal apresentou obrigações referentes ao tratamento de dados fora do território nacional, proteção aos direitos civis na aplicação de ação algorítmica para perfilamento de usuários, transparência das plataformas digitais, com divulgação de relatórios periódicos de conduta e proteção ainda mais restritiva a menores.

Leone de Castris (2022) pontua que as legislações propostas para as plataformas digitais sempre se referem à necessidade de aumento na transparência, porém, o termo na maioria das vezes é tratado de forma vaga. Não há entre os legisladores uma compreensão e definição de padrões de transparência. Enquanto as propostas não forem unificadas, fica mais complexa a operacionalização do conceito. Isso porque no princípio este conceito estava centrado no poder econômico que a opacidade dava às plataformas, porém, com o passar do tempo, revelou-se que há também uma concentração de poder político nesta questão da obscuridade com que os dados são tratados. A crítica sobre a falta de transparência se torna vazia pela falta de parâmetros, que precisam ser mais bem delineados pelos legisladores.

5.3.2.8 Projetos de Lei referentes à privacidade e segurança

A privacidade de crianças era o foco do projeto de Lei apresentado, em outubro de 2013, pelo deputado John J. Duncan Jr. sob o título de Forbidding Advertisement Through Child Exploitation Act – FACE Act (H.R. 2645). O projeto proibia plataformas digitais de divulgarem imagens de menores, utilizadas para identificação de perfis online, para propaganda. O projeto tinha o objetivo de combater a exploração

comercial infantil em anúncios na rede. Caberia à FTC fiscalizar as plataformas e aplicar sanções em casos de irregularidades identificadas.

Em 1989, a Unicef fez uma Convenção sobre os direitos das crianças. Van Der Hof *et al.* (2020) demonstram que no ciberespaço estes direitos infantis não vêm sendo respeitados. Nas plataformas digitais há uma miríade de formas de exploração infantil, atentando ao tema desta tese, a utilização dos dados das crianças para encaminhamento de conteúdo e manufatura de produtos é um deles. Constantemente as crianças são expostas a uma atitude de consumo desenfreada, com modelos de atração difíceis de serem burlados por quem ainda está aprendendo a lidar com a vida. O desenvolvimento do conceito de privacidade, inclusive, é bastante prejudicado pela forma como as plataformas digitais agem.

Em setembro de 2018, o deputado Luke Messer (PR – IN) apresentou o projeto de Remove Explicit Material Offensive to Victims Expeditiously Act - REMOVE Act (H. R. 6917). O instrumento regulatório obrigaria a FTC a criar um site, no qual o usuário pudesse identificar se haveria alguma imagem sua, de cunho sexual, que tivesse sido divulgada sem o seu consentimento. A partir desta identificação, o usuário poderia exigir a imediata remoção da imagem. Os provedores de serviços online seriam obrigados a manter políticas de remoção de imagens sexuais não consentidas e estarem disponíveis a notificações para este tipo de ação.

O senador Joe III Machin, propôs, em setembro de 2020, um projeto de Lei que previa o monitoramento de transmissões suspeitas em plataformas digitais. O projeto de Lei See Something, Say Something Online Act (S.4758) tornaria obrigatório às plataformas digitais a comunicação de possíveis transmissões suspeitas que pudessem auxiliar em investigações de contraespionagem ou relacionadas a terrorismo internacional. De acordo com o texto, transmissão suspeita seria considerada uma postagem, mensagem, comentário, *tag*, transação pública ou privada, e qualquer outro tipo de conteúdo emitido por usuário que cometa, facilite ou incite a prática de crime grave.

Os funcionários das plataformas digitais seriam obrigados, em caso de contato com transmissão suspeita, a enviar um relatório, no prazo de no máximo 30 dias, relatando a ação. No caso de identificação de ameaça iminente, a comunicação deveria ser feita por telefone à autoridade policial. O texto não foi aprovado e novamente o parlamentar apresentou no ano seguinte, sem alterações (S.27).

A preocupação com o contato dos usuários com conteúdo terrorista também era a preocupação do deputado Tom Malinowski (PD – NJ), que apresentou o projeto de Lei Protecting Americans from Dangerous Algorithms Act (H.R.8636). A proposta previa a responsabilização de plataformas digitais que de algum modo disseminassem conteúdo terrorista por meio de perfis de filiação criados a partir de algoritmos. A proposta trazia ainda a possibilidade de responsabilização pela não remoção de material que ia contra os direitos civis dos cidadãos estadunidenses. A proposta foi reapresentada pelo mesmo autor em 2021 (H.R.2154), com apoio do senador Ben Ray Lujan (PD – NM), que fez a introdução da proposta no senado (S.3029).

O risco de ser vítima de fraude foi tratado no projeto de Lei Online Dating Safety Act (H.R.8946), do deputado David G. Valadao (PR – CA). De acordo com o texto, da proposta apresentada em setembro de 2022, as plataformas digitais que promovem encontros online deveriam enviar notificações de segurança para seus usuários, assim como instruir a proibição de tais ações na plataforma. Além disso, a identidade dos usuários deveria contar com uma forma de verificação. O texto previu também uma forma de que um usuário pudesse denunciar indivíduo que estivesse tentando aplicar golpes via plataforma.

Preocupada com o vício de uma boa parcela da população em redes sociais, a senadora Amy Klobuchar (PD – MN) apresentou, em fevereiro de 2022, o Nudging Users to Drive Good Experiences on Social Media - Social Media NUDGE Act (S.3608). O projeto de Lei propunha a redução da ação de seleção e direcionamento dos algoritmos das plataformas digitais e incentivava estudos científicos na tentativa de identificar meios de minimizar o vício em redes sociais no ciberespaço. A congressista propôs algumas ações algorítmicas neutras, que chamou de agnósticas. Estas medidas incluiriam: implementação de controladores de tempo de uso, com alertas aos usuários sobre período de permanência; telas em escala de cinza e não com luz azul, que são mais viciantes; utilização de *tags* e alertas que obriguem o usuário a revisar seu conteúdo antes de postar; solicitações às plataformas para identificação de conteúdo direcionado, seja por impulsionamento ou anúncio; e, limite para produção e compartilhamento de conteúdo, por usuário, durante um determinado período. As ações devem ser implementadas pela Federal Trade Commission.

Spencer (2022) destaca que a ênfase em ações técnicas, como alerta de tempo em tela, ou tons de cinza é uma tentativa de os legisladores do NUDGE Act evitarem o embate com a liberdade de expressão, presente na 1ª Emenda da Constituição

Norte Americana. Keller (2021) denota que ferramentas que limitam o número de vezes que um conteúdo será mostrado por hora vão acabar atingindo não apenas conteúdo nocivo, mas também informações válidas. Interessante seria que a Lei previsse a remoção de conteúdo, que de acordo com a Lei é ilegal, como terrorismo, por exemplo. Mcdermott (2023) sublinha que a Lei vai rivalizar com a liberdade de expressão, exatamente porque seu foco é o combate à disseminação de desinformação, resultado da produção e compartilhamento de material malicioso, porém, isso seria impossível sem o tratamento do conteúdo como um todo.

No mês de junho de 2022, o deputado David Schweikert (PR – CA) trouxe novamente à discussão a proteção dos dados dos usuários de internet, com seu projeto de Lei User Data Protection Act (H.R.4240). O parlamentar propôs o estabelecimento de requisitos mínimos de segurança para coleta, tratamento e armazenamento de dados dos usuários. A proposta citava a ação dos *cookies*, que monitoram cada ação do usuário na rede e instituía a obrigatoriedade de consentimento para rastreamento, proibição de bloqueio de sites por não consentimento de coleta de dados, veto para coleta oculta por meio de pixels de imagens e compartilhamento de dados com terceiros sem anuência do usuário.

O projeto de Lei reconhecia o usuário como proprietário de seus dados e por isso ele deveria ser informado sobre a finalidade de utilização das informações, inclusive aferição financeira para compartilhamento. Qualquer mudança na forma de coleta e tratamento, assim como aferição financeira pelas informações deveria ser comunicada. Para Almeida, Shmarko e Lomas (2022) o escopo do projeto de Lei já estaria desatualizado. Isso porque na Europa e Inglaterra o que se vem discutindo é uma questão mais abrangente de coleta de dados, que inclui o reconhecimento facial, amplamente utilizado por empresas de tecnologia em equipamentos eletrônicos e que pode ser empregado em ações de segurança pública. As polícias estaduais estadunidenses vêm, inclusive, tentando comprar sistemas de reconhecimento facial para esta finalidade, porém, a Amazon informou que só faria a venda destes sistemas depois da aprovação de Leis regulatórias federais que tratassem do assunto, para evitar responsabilidades futuras.

Altman (2023) concorda que a ação governamental de regulação das políticas de privacidade precisa avançar rapidamente porque a IA não para, ao contrário, a evolução tecnológica está mudando completamente o quadro de diversas áreas, como a educação, por exemplo. Não há como parar e esperar que as normas regulatórias

sejam implementadas, porém, os governos precisam estar atentos e avançarem rapidamente nas discussões regulatórias para evitar riscos futuros com a utilização da tecnologia na vida diária dos cidadãos.

De acordo com o projeto, a FTC ficaria responsável pela fiscalização do cumprimento das normas, assim como punição de possíveis irregularidades, que poderiam resultar em multas e outras penalidades. Os procuradores estaduais também poderiam agir em ações civis públicas sempre que sentirem que os direitos de cidadãos de suas localidades forem atingidos. A ações incluem acordos de *compliance*, pedido de indenizações e multas civis. Nestas ações a FTC teria de ser comunicada e ouvida.

5.3.2.9 Projetos de Lei referentes à segurança

Apresentado em junho de 2007, o projeto de Lei Counter Spy Act (S. 1625), do senador Mike Pryor (PD – AR), propôs a criminalização de quem fizesse a instalação de software em equipamento alheio com o intuito de roubar dados dos usuários. A instalação de qualquer programa em computador de usuário só seria autorizada mediante consentimento. Condicionaria ainda a instalação de software de coleta de dados única e exclusivamente para melhorar a experiência do usuário de plataformas digitais. Além disso, anúncios só poderiam ser mostrados durante a navegação em uma página e não como adware, que se trata de um programa que vai lançando propaganda em tela, sem que o usuário tenha como controlar a exibição.

Como já foi mostrado, a exploração sexual infantil online já era uma preocupação na legislatura de 2007-2008, e alguns projetos com esta temática foram anexados à Lei Broadband Data Improvement Act (Law Nº 110-385 – 10/10/2008). Alguns projetos, porém, não chegaram a ser anexados, caso da proposta do deputado Christopher Carney (PD – PA), introduzido em outubro de 2007, sob o título Responsible and Effective Solutions for Children Using and Entering Online Services Act (H.R.3850). O projeto de Lei trazia a possibilidade de que os dados de usuários de plataformas digitais pudessem ser utilizados em investigações de combate à pornografia infantil. As plataformas digitais não seriam consideradas responsáveis, caso de boa-fé denunciassem atividade suspeita relacionada a este tipo de crime e colaborassem com evidências para o processamento dos crimes. O texto criava ainda uma via de mão dupla entre os serviços de internet e o Nacional Center of Missing &

Exploited Children (NCMEC), que poderia enviar imagens de pornografia infantil para evitar que continuassem a ser distribuídas.

Voltando à temática do combate à pornografia infantil, em novembro de 2009, o deputado Bart Stupak (PD – WI) propôs exigir de plataformas digitais com conteúdo adulto, que fossem obrigadas a fazer checagem etária antes da exibição do conteúdo. O projeto Online Age Verification and Child Safety Act (H.R.4059) ainda trazia a proibição de comercialização de produto proibido para menores, sem um mecanismo de verificação etária antes da transação. Negociações por meio de moeda eletrônica também estavam listadas entre as proibições do mecanismo legal. A fiscalização ficaria a cargo da FTC, com aplicação de multas e sanções por irregularidades constatadas.

Depois de um período sem que o assunto fosse discutido nas casas legislativas, ele voltou à cena regulatória em 2020 com o projeto de Lei Eliminating Abusive and Rampant Neglect of Interactive Technologies Act – EARN IT Act (S. 3398), da senadora Lindsey Graham (PR – SC), que foi posteriormente apresentado também na câmara pela deputada Sylvia Garcia (H.R.8454). A proposta previa a criação de uma comissão nacional que fizesse a prevenção à exploração sexual infantil online. A comissão teria jurisdição para atuar em todos os serviços interativos de computador, como previsto na seção 230 da Communication Act de 1934, promulgada como parte da Communication Decency Act de 1996.

Caberia à comissão desenvolver parâmetros e práticas para que as plataformas digitais pudessem implementar para reduzir, prevenir e responder às ameaças de exploração sexual infantil, que incluíssem sedução, aliciamento, tráfico e abuso, com divulgação de material online. De acordo com Whiting (2023) a tentativa de emplacar o projeto de Lei foi corroborada pelo aumento no número de denúncias de casos de exploração sexual infantil. Relatórios do National Center for Missing & Exploited Children confirmaram que o número de arquivos contendo exploração sexual infantil passou de 1.1 milhão em 2014 para 19.9 milhões em 2019.

A comissão seria composta por 19 integrantes governamentais, com membros do departamento de segurança, câmara e senado. Estes integrantes precisariam ter como qualificações a experiência no combate à exploração sexual infantil, aplicação da Lei, acusação judicial, apoio às vítimas, respeito aos direitos individuais e conhecimento em tecnologia, visando a proteção de crianças online. As práticas deveriam ser adaptadas ao tipo de serviço ofertado pelas plataformas digitais de

acordo com suas funções: rede social, armazenamento de dados, compartilhamento de conteúdo e hospedagem de sites.

Plataformas digitais precisariam se comprometer com as melhores práticas e ainda garantir que parceiros terceirizados também concordassem. As ações propostas deveriam levar em conta: custo de implementação; impactos de competição, qualidade do serviço, privacidade e segurança do usuário; impacto na investigação e punição de culpados. As plataformas seriam incentivadas a relaxarem as regras de criptografia para identificar possíveis distribuidores de material abusivo, com oferta voluntária de provas pelas empresas ao governo (H.R.8454).

O problema da exploração sexual infantil ainda foi base de vários projetos de Lei posteriores. Como foi o caso do Eliminate Network Distribution of Child Exploitation Act – END Exploitation Act (H.R.5376 / S.3007) proposto pelo deputado Anthony Gonzalez (PR – OH) e a senadora Marsha Blackburn (PR – MS), em dezembro de 2019. A proposta impunha às plataformas digitais a obrigatoriedade de manter seguro, por até 180 dias, conteúdo denunciado pela CyberTipline do NCMEC, sobre exploração sexual infantil. O projeto previa ainda que as plataformas fizessem esta guarda do material de forma voluntária também.

A mesma exigência, de guarda de material de denúncia da CyberTipline da NCMEC, com relação à exploração sexual infantil, previa projeto de Lei do senador Ron Wyden (PD – OR) e da deputada Anna G. Eshoo (PD – CA), Invest in Child Safety Act (S.3629 / H.R.6752), apresentado em maio de 2020. O projeto voltou a ser apresentado em 2021 (S.223 / H.R.807) sem alterações.

Uma das preocupações de alguns pesquisadores seria a imposição de que plataformas agissem como agentes de investigação, o que as tornaria braços do Estado no cotidiano dos usuários. A quarta emenda da constituição estadunidense prevê que toda busca exige mandado, emitido por juiz, sob a égide da provável execução de crime. A busca e disponibilização de material pelas plataformas digitais, sem mandado, poderia ser considerado em corte como prova inadmissível, pelo não cumprimento do devido processo legal. Além disso, esta prática poderia incentivar governos totalitários a exigirem de plataformas estadunidenses o mesmo tipo de acesso para identificar e punir minorias, como a comunidade LGBTQIA+ (Schumer, *et al.*, 2023).

O projeto sinalizou, porém, que as regras não poderiam impedir a punição civil das plataformas digitais pela violação de direitos de crianças e adolescentes, como o

contato com material pornográfico ou que tivessem sido vítimas de exploração. Para o projeto de Lei, pornografia infantil deveria ser reconhecida como qualquer material de abuso sexual infantil. O projeto de Lei propunha ainda a atualização dos termos em mais de 20 instrumentos legais.

Pfefferkorn (2022) alerta que o projeto propõe retirar parte da imunidade das plataformas pelo material de abuso sexual divulgado em seus serviços. Atendendo às práticas propostas, as plataformas estariam em conformidade com a Lei, ficando livres de ações penais. As plataformas só poderiam responder por danos civis causados a menores vítimas de exploração sexual infantil online ou que tiveram contato com este tipo de material. Monea (2022) destaca que o projeto incentiva as plataformas digitais a moderar qualquer tipo de conteúdo sexual destinado a jovens, mesmo que seja educativo, de profissionais do sexo ou retrate minorias, o que poderia ser uma abertura ainda maior para censura da temática na internet.

Atividades ilegais na rede também entraram na agenda regulatória. Em julho de 2008, o deputado Robert Scott (PD – WA) apresentou o projeto E-fencing Enforcement Act (H. R. 6713), que propunha a mudança do código criminal dos EUA para impor obrigações às plataformas digitais que divulgassem informações sobre os responsáveis por anúncios de produtos, fruto de roubo. Além disso, obrigava as plataformas a negar acesso a vendedores de alto volume de produtos que pudessem levantar a suspeita de serem roubados. As plataformas seriam obrigadas a reter informações dos vendedores, fornecer estes dados quando solicitado, remover conteúdo online e estariam sujeitas a ação civil em caso de descumprimento da ordem. O projeto não evoluiu na legislatura 110th e foi novamente apresentado em fevereiro de 2009 (H. R. 1166), sem alteração de texto.

O senador Patrick Leahy (PD – VT) apresentou em setembro de 2010 o projeto de Lei Combating Online Infringement and Counterfeits Act (S.3804), que autorizava o procurador-geral a processar sites de comercialização de produtos ilegais, ou que infringem Lei de direitos autorais, mesmo quando hospedados fora dos EUA, confiscando o domínio. Para isso, exigiria das plataformas digitais que cumprissem ordens judiciais evitando que atividades ilegais continuassem em território estadunidense, também concederia imunidade às empresas que voluntariamente evitassem atividade criminosa online.

Em maio de 2011, o senador Leahy voltou a apresentar proposta com temática idêntica, mas sob novo título Preventing Real Online Threats to Economic Creativity

and Theft of Intellectual Property Act - PROTECT IP Act (S.968). O texto foi completamente modificado com relação à proposta anterior, que tratava da responsabilização das plataformas digitais por associação a atividades ilegais nos EUA, pela hospedagem de conteúdo de terceiros, porém, o objetivo da norma permaneceu o mesmo. Um detalhamento do texto deixou ainda mais claro que para serem responsáveis por conteúdo de terceiros, que praticassem atividade ilegal, bastava a divulgação de link, índices ou ponteiros de acesso ao domínio de comercialização ilegal. Além disso, a divulgação dos produtos, via anúncio online, também foi enquadrada na norma como forma de associação.

Posteriormente relacionada ao projeto do senador Patrick Leahy (PD – VT) foi a proposta do deputado Lamar Smith (PR – TX), que previa inflexibilidade para crimes de pirataria em rede sob o título Stop Online Piracy Act (H.R.3261). O instrumento legal autorizaria o procurador-geral a pedir a cassação de registro de site estrangeiro que facilitasse a pirataria de material audiovisual, bens e serviços. O projeto previa a compensação de quem detinha os direitos autorais de tais produções e estava sendo lesado. As plataformas digitais deveriam atender ordens judiciais de remoção de conteúdo, assim como poderiam voluntariamente retirar do ar material fruto de pirataria. Havia, inclusive, uma cláusula para falsificação de medicamentos e informações de saúde.

Em dezembro de 2011, o senador Ron Wyden (PD – OR), propôs o Online Protection and Enforcement of Digital Trade Act – OPEN Act (S.2029), que previa a criminalização de plataformas digitais estrangeiras que facilitassem a comercialização de produtos e serviços ilegais em território estadunidense. O foco do texto estava principalmente na ofensa a direitos autorais e marcas protegidas. Podem ser responsabilizados serviços de publicidade online e financeiros, que trabalham em associação a tais sites. Ambos só receberiam imunidade em caso de colaboração com medidas judiciais que cessassem a ação ilegal. O projeto foi introduzido na câmara, pelo deputado Darrell E. Issa (PR – OH), em janeiro de 2012 (H. R. 3782).

Em junho de 2018, a senadora Daianne Feinstein apresentou o projeto Bot Disclosure and Accountability Act (S. 3127), prevendo que as plataformas fossem obrigadas a identificar a utilização de *bots* em ações de disseminação de conteúdo online. O projeto não passou na legislatura 115, e foi novamente introduzido em julho de 2019 no Senado (S. 2125), e em setembro na Câmara (H. R. 4536), pela deputada Elissa Slotkin (PD – MI). Para as autoras, os *bots* expõem os usuários a erros, porque

são criados para simular a ação humana, mas fazem disparo de informações em massa. O maior risco, segundo o projeto, residiria na possibilidade de utilização destes *bots* em campanhas difamatórias e de desinformação durante processos eleitorais. Os *bots* não seriam proibidos, apenas identificados.

Em julho de 2019, foi introduzido pelo senador Josh Hawley (PR – MO) o projeto de Lei Social Media Addiction Reduction Technology Act – SMART Act (S. 2314). A proposta da Lei exigia que as plataformas de mídias sociais digitais utilizassem medidas de mitigação de práticas psicológicas que interferissem no poder de escolha dos usuários ou favorecessem comportamento adicto. A ideia seria de implementar ações que dessem aos usuários maior poder de escolha, com menos manipulação, aumentando a possibilidade de controle do tempo gasto nas plataformas digitais. A proposta previa a proibição de barra de rolagem infinita; play automático para conteúdo; eliminação do ponto final após o consumo de um conteúdo; utilização de algoritmo de recomendação, sem consentimento; recompensas por tempo gasto ou engajamento com a plataforma digital.

Ações contrárias à norma podem ser punidas com multas e restrições da FTC. A execução fica a cargo dos advogados gerais dos estados, que também podem mover ações civis públicas caso entendam que os direitos de residentes de suas localidades estejam sendo prejudicados. Antes da apresentação da ação civil pública, o advogado do estado deve enviar à FTC um comunicado por escrito com a violação em questão. Caso decida intervir, a FTC precisa ser ouvida (S.2314).

Birnbaum (2019) pontua que a norma é extremamente invasiva porque interfere no design dos serviços. Faz parte do Twitter, Facebook, Instagram a barra de rolagem infinita ou o autoplay do Youtube. As empresas teriam que desenvolver outros tipos de produtos, de acordo com a norma. Há muita diferença na forma como crianças, adolescentes e adultos fazem uso das redes sociais digitais. Normas que tratassem do problema por faixa etária poderiam ter melhor aceitação.

Já Sapone (2021) observa que a proposta falha em não trazer dados estatísticos que comprovem os malefícios das redes sociais. Redes sociais digitais têm sido consideradas mais viciantes que cigarro ou álcool, em média os estadunidenses checam seus celulares ao menos 100 vezes ao dia e permanecem pelo menos 144 minutos diariamente em plataformas digitais. No geral, as plataformas digitais desenvolveram seus serviços utilizando a dopamina, que é o hormônio da recompensa, do prazer. Quanto mais o usuário tem contato com a satisfação, em

vídeos ou conteúdos curtos, mais ele quer. A dopamina está no centro de qualquer comportamento adicto, porém, os males causados pelas redes sociais ainda não foram reconhecidos pelo Statistical Manual of Mental Disorders.

O maior equívoco apontado por Sapone (2021) na proposta legislativa reside na tentativa de regular o usuário e não a plataforma. Já que é o tempo que é a forma de consumo do conteúdo que está em xeque e por isso a resistência à Lei segue grande. Afinal, atinge novamente a Primeira Emenda da Constituição, no quesito liberdade do indivíduo. Para as plataformas digitais, se a Lei passasse seria um pesadelo logístico, por conta do curto espaço de tempo para colocá-la em prática. E ainda, para os não viciados, toda a experiência do usuário estaria comprometida.

Apresentado Nos anos de 2019 e 2021, o projeto de Lei Protecting Local Authority and Neighborhoods Act – PLAN Act (H.R.4232 / H.R.1107), do deputado Ed Case (PD – HI), trouxe à discussão a facilitação de locação de imóveis via plataformas digitais, em desacordo com Leis estaduais do mercado imobiliário. De acordo com o texto, as plataformas poderiam ser consideradas responsáveis por conteúdo de terceiros, quando avisadas de *posts* em desacordo com Leis locais e estaduais, em oferta de imóveis para locação, não fizessem a retirada do conteúdo do ar.

O projeto de Lei National Commission on Online Platforms and Homeland Security Act (H.R.4782), do deputado Bennie G. Thompson (PD – MS), propunha a criação de uma comissão que analisasse o conteúdo das redes sociais digitais, em busca de possíveis riscos à segurança nacional. Caberia à comissão identificar, examinar e relatar possíveis ameaças de promoção ou apoio à violência, ou até mesmo campanhas secretas de influência de estados estrangeiros em ambiente estadunidense.

A análise também trataria de organização ou divulgação de atos de terrorismo interno e externo. A comissão deveria ser composta de 12 indivíduos apontados por comitês de segurança da câmara e senado, com experiência prévia em tecnologia. Caberia à comissão analisar a moderação de conteúdo das plataformas, se estariam obedecendo aos Princípios de Santa Clara. Durante o período de análise, as plataformas poderiam ser obrigadas a fornecer informações, como complemento a estudos científicos que tratassem dos riscos de segurança nacional no ambiente digital.

A comissão teria o poder de intimar e ouvir testemunhas, a partir destas oitivas elaborar relatórios e documentos na extensão necessária para identificação das

ameaças. As informações levantadas a partir destes depoimentos não poderiam ser compartilhadas com agências de segurança federal, estadual, local ou internacional. Encontros públicos deveriam ser marcados para divulgação de relatórios. O compartilhamento de estudos e pesquisas deveria ter divulgação de versão que fizesse a anonimização dos dados pessoais de usuários. A partir das análises, caberia à comissão elaborar normas regulatórias que deveriam ser colocadas em prática pelas plataformas digitais.

Na mesma linha de ação, foi proposto pelo deputado Max Rose (PD – NY) o projeto de Lei Raising the Bar Act (H.R.5209), em novembro de 2019. A proposta de Rose previa uma moderação voluntária de conteúdo terrorista, num estudo piloto feito por uma instituição com experiência comprovada em terrorismo doméstico, internacional, cibersegurança, privacidade ou tecnologia da informação. As plataformas digitais assinariam um acordo de cooperação. O trabalho deveria ser feito durante quatro semanas seguidas. A instituição executora do teste de moderação deveria receber das plataformas digitais qual tratamento era dado a conteúdo terrorista de acordo com seus termos de serviço. A instituição criaria padrões de moderação para este tipo de conteúdo, com notificação das plataformas, sinalizadores confiáveis e após a execução das quatro semanas de teste, elaboraria um relatório com os resultados.

Lowry (2020) constata que as preocupações dos legisladores estadunidenses residem não apenas nas ações terroristas que podem ser potencializadas via redes sociais digitais, mas também na influência de governos estrangeiros em campanhas eleitorais. Prabhu (2020) denota que conservadores e progressistas concordam que algo precisa ser feito no sentido de proteger a nação contra interferências internacionais em campanhas de desinformação em conteúdo propagado via redes sociais, o que pode causar discordância é o nível de interferência governamental na manutenção de liberdades civis e individuais de seus cidadãos no processo regulatório. As ações legislativas do congresso neste tema só tiveram início após a denúncia de influência da Rússia nas eleições de 2016.

O medo da influência estrangeira no governo estadunidense fez o senador Josh Hawley (PR – MO) apresentar o projeto de Lei No TikTok on Government Devices Act (S.3455), em março de 2020. A proposta foi apoiada e introduzida na câmara pelo deputado Ken Buck (PR – NY) (H.R.6896). Como o nome já trouxe, a proposta era de que nenhum aparelho de comunicação do governo estadunidense tivesse instalado o

app TikTok, da empresa chinesa ByteDance Limited. A utilização do app só seria permitida em casos de exceção, para investigação e seu uso deveria ser feito com medidas mitigatórias para evitar monitoramento estrangeiro. O projeto não passou e foi novamente apresentado em 2021 (S.1143 / H.R.2566), pelos mesmos parlamentares.

O aplicativo chinês foi ainda tema de outros três projetos de Lei, a deputada Lisa C. MacClain, propôs em maio de 2021, o Anti-CCP Espionage via Social Media Act - ACES Act (H.R.3057). A proposta era semelhante ao projeto de Lei anteriormente citado. Foi acrescido ao texto um pedido de investigação de como usuários estadunidenses vinham negociando com a empresa chinesa. Em setembro de 2022, o deputado Dusty Johnson (PR – SD) apresentou o Block the Tok Act (H.R.8772) que proibia o app chinês de acessar os dados dos usuários estadunidenses. Além disso, ainda reforçava a proibição de *download* do app em instalação de segurança e militares. No final de 2022, o deputado Mike Gallagher (PR – WI) e o senador Marco Rubio (PR – FL) introduziram o projeto Averting the National Threat of Internet Surveillance, Oppressive Censorship and Influence - ANTI-SOCIAL CCP Act (S.5245 / H.R.9508), proibindo o app de conduzir transações financeiras nos EUA, além de ser proibido em instalações militares.

Em outubro de 2019, foi introduzido pelo deputado Jesus Garcia o projeto de Lei Keep Big Tech Out Of Finance Act (H.R.4813), que propunha a proibição de associação das *BIG Techs* com instituições financeiras ou que funcionassem como uma. A proposta dava prazo de um ano para empresas de tecnologia que já estivessem operando como instituições financeiras, ou associadas a uma, que encerrasse tais atividades. Pelo texto, também seria proibida a operação de moedas digitais pelas plataformas. Infratores estariam sujeitos a multa de US$ 1 milhão por dia. Segundo o projeto, todo o sistema financeiro estadunidense tem regulação própria e operar fora dele seria um crime.

Encerrando o ano de 2019, a proposta Combating Online Wildlife Trafficking Act (H.R.5398) foi introduzida pelo deputado Earl L. Carter requerendo das plataformas digitais uma ação conjunta com agências de segurança dos EUA para tratar do combate ao tráfico de animais, em conteúdo postado na rede. Segundo o texto, uma força-tarefa trabalharia em conjunto com as plataformas digitais para elaborar métodos de identificação de conteúdo referente a tráfico de animais na web.

A proposta não passou na primeira apresentação e foi reintroduzida em 2021 (H.R.1546), porém, novamente não evolui no processo legislativo.

Em abril de 2020, o deputado Adam Kinzinger (PR – IL) apresentou dois projetos para combater as contas falsas nas redes sociais. O Social Media Accountability and Account Verification Act (H.R.6586) que tinha a intenção de obrigar as plataformas digitais a excluírem contas falsas. E o Social Media Fraud Mitigation Act (H.R.6587), que previa a criminalização de quem abrisse uma conta falsa em rede social. Ambos os projetos foram reintroduzidos no ano seguinte (H.R.4653 / H.R.4654), mas também não passaram da introdução na Câmara.

A senadora Lindsey Graham (PR – SC) propôs, em setembro de 2020, um projeto de Lei que previa a criação de um órgão para tratar das pequenas disputas sobre direitos autorais. O Online Content Policy Modernization Act (S.4632) propunha a criação do Copyright Claims Board que seria um fórum alternativo para pequenas demandas de direitos autorais. Neste âmbito as disputadas estariam restritas a até US$ 30 mil. A proposta ainda trazia no seu bojo a responsabilização das plataformas digitais em caso de editoração ou modificação de conteúdo de terceiros e ainda pela mudança de layout ou aparência de *post* de usuário.

O apoio a conteúdo ilegal na rede tornaria as plataformas digitais responsáveis pelo material postado, era esta a proposta do deputado W. Gregory Steube (PR – FL), que apresentou o projeto de Lei Curbing Abuse and Saving Expression In Technology Act – CASE-IT Act (H.R.8719), apresentado em outubro de 2020. Além do conteúdo ilegal, o texto trazia a possibilidade de responsabilização das plataformas digitais por permitirem o contato de um adulto, com menor, em atividade de exploração sexual. A proposta previa a perda de imunidade das plataformas pelo prazo de um ano, após a constatação de irregularidade prevista na regulação. Somada à proposta, estava a possibilidade de responsabilização também, quando um provedor dominante restringisse ou impedisse a propagação de conteúdo de terceiros, com previsão de multa de US$ 500 mil por ação.

Ainda na linha de punição das plataformas por manterem conteúdo que envolvam tráfico de materiais ou exploração sexual infantil, a senadora Kelly Loeffler (PR – GA) propôs o projeto de Lei Holding Sexual Predators and Online Enablers Accountable Act (S.5012), em dezembro de 2020. O infrator estaria sujeito à pena de 25 anos e multa, que poderiam ser aumentados em caso de tratar-se de exploração sexual infantil.

O combate ao terrorismo foi o tema central do projeto de Lei No Social Media Accounts for Terrorists or State Sponsors of Terrorism Act (H.R.1543), proposto pelo deputado Andy Bar, em março de 2021. O texto trazia a exigência de que o Presidente dos EUA proibisse as plataformas de mídia social, que tivessem mais de 100.000 usuários ativos, de disponibilizar serviços a indivíduos identificados como membros de organizações terroristas ou funcionários impedidos de governos que apoiassem este tipo de ação.

O deputado Lance Gooden (PR – TX), em parceria com o senador Josh Hawley (PR – MO), apresentou uma proposta que cria um direito privado de ação contra uma empresa de mídia social quando um indivíduo, menor de 16 anos, sofre lesão corporal ou danos à saúde mental que pode ser atribuível, no todo ou em parte, ao uso do site de uma empresa de mídia social, aplicativo online ou aplicativo móvel. O projeto Federal Big Tech Tort Act (H.R.5449 / S.2917) foi introduzido em setembro de 2021. As empresas de tecnologia poderiam ser obrigadas a pagar indenizações e custas advocatícias.

A busca por um ambiente seguro online era o foco da proposta do deputado Gus M. Bilirakis (PR – FL), que apresentou, em fevereiro de 2022, o projeto de Lei Cooperation Among Police, Tech, and Users to Resist Exploitation Act – CAPTURE Act (H.R.6755). A proposta exigia do controlador geral dos EUA a instituição de uma cooperação entre forças policiais e empresas de mídias sociais, na elaboração de um estudo sobre o conteúdo ilegal postado na web. O estudo deveria apresentar iniciativas já concretizadas de sucesso e fracasso em cooperações desta natureza, de quais formas as redes sociais vêm lidando com conteúdo ilegal na rede e com propostas de normas regulatórias que possam contribuir para o combate a este material online, estabelecendo ainda um único ponto de contato entre as empresas e as forças de segurança.

Em março de 2022, o deputado Madison Cawthorn (PR – NC) introduziu na câmara o projeto de Lei No Publicity for Terrorists Act (H.R.6918). De acordo com o texto, as plataformas digitais deveriam remover usuários identificados como membros de organizações terroristas. As empresas também seriam obrigadas a enviar relatórios trimestrais sobre transações financeiras intermediadas em seus ambientes. A proposta de Lei institui a Securities and Exchange Commission como órgão para o qual o relatório deveria ser enviado e, portanto, seria o ponto de fiscalização de cumprimento do regulamento.

A segurança nacional dos EUA estaria em risco se cidadãos da alta cúpula do poder chinês pudesse utilizar as redes sociais de empresas estadunidenses. Este foi o mote principal do projeto de Lei proposto pelo Brian J. Mast (PR – MI), em junho de 2022, intitulado China Social Media Reciprocity Act (H.R.8041). De acordo com o texto, as plataformas de mídias sociais estadunidenses teriam que se negar a prestar serviço a cidadãos e entidades listados como especialmente designados na República Popular da China. Caso mantivessem os serviços, tais empresas estariam sujeitas a penalidades como multas.

Ainda na linha da segurança interna e combate a ameaças internacionais foi apresentado o projeto de Lei Countering Foreign Malign Influence Act (H.R.8409), do deputado Sean Patrick Malone, em julho de 2022. De acordo com o texto, o regulamento previa mecanismos ao Social Media Data and Threat Analysis Center, para analisar ameaças e propor ação às plataformas de mídias sociais no sentido de bloquearem pessoas e instituições que oferecem risco à segurança nacional estadunidense. A ação faria a análise da ação de *bots*, de contas falsas, de mídia manipulada, campanhas de desinformação e perfis falsos.

A prevenção à ação de quadrilhas internacionais, que utilizam as redes sociais para recrutar moradores dos EUA para a prática de atividade criminosa no país, em suas fronteiras ou nações vizinhas, foi tratada no projeto de Lei Combating Cartels on Social Media (S.4963), proposto pela senadora Krysten Sinema, em setembro de 2022. A proposta tratava de uma cooperação entre o DHS, polícias e departamento de justiça, assim como, operadores das plataformas digitais, para a criação de um sistema de informações para denúncias de ações das quadrilhas internacionais nos serviços online.

As plataformas digitais deveriam facilitar acesso ao DHS e aos serviços de segurança para investigações, assim como corporações de outras nações para identificação de atividade criminosa que utilizam as plataformas digitais em ações de recrutamento de pessoal. Fariam parte da força tarefa regulatória membros de controle de fronteira, do FBI, do DEA, de direitos civis, privacidade e direitos humanos, secretarias de Ciência, Tecnologia e IA. O projeto atingiria plataformas de mídias sociais, serviços de mensagem instantânea, serviços de streaming e serviços de aplicativos. O objetivo seria o combate ao tráfico de drogas, pessoas e armas, assim como ação terrorista no território estadunidense.

Di Nicola (2022) observa que a sociedade da informação criou um novo quadro do crime organizado, sendo ele distribuído entre ações feitas apenas na rede, com outros grupos que transitam entre o online e o offline, com aqueles que ainda trabalham de forma analógica, porém, ainda assim, utilizam a internet principalmente para comunicação. O crime organizado digital vem trabalhando desde a década de 1990 na descoberta de novas aplicações da tecnologia para suas práticas delitivas. A utilização mais comum é de recrutamento, como a Lei prevê, mas há ainda ação de aumento da rede de contatos de compradores, relacionamento com outras quadrilhas, anúncio de produtos ilícitos, entre outras aplicações.

5.3.2.10 Projetos de Lei referentes à liberdade de expressão, privacidade e segurança

No mês de maio de 2022, foi apresentado primeiramente no Senado, e na sequência na Câmara, o projeto de Lei de regulação das plataformas digitais nomeado de Digital Platform Commission Act (S.4201 / H.R.7858). O projeto previa o estabelecimento de um órgão federal, a Federal Digital Platform Commission (FDPC), que funcionaria como uma agência regulatória. Ela seria responsável pela criação de um arcabouço regulatório para as plataformas digitais que fosse conveniente e necessário ao interesse público, proporcionando à população dos EUA acesso cível, econômico e educativo à rede; acesso aos serviços governamentais e de segurança pública; concorrência de mercado e inovação; combate à concentração de atividades em oligopólios tecnológicos; diversidade de visões ideológicas; proteção de consumidores contra práticas abusivas e garantia de atividades algorítmicas justas, transparentes e seguras.

Para Feld (2019), a criação de uma agência regulatória é uma forma já conhecida de fomento do arcabouço legal para as plataformas digitais, visto que este foi o caminho escolhido para outros setores, como Telecomunicações, Indústria Farmacêutica, Transporte, entre outros fundamentais para economia estadunidense. No caso das plataformas digitais, a falta de regulação tornou o quadro num desafio regulatório. As empresas de tecnologias são oligopólios que causam inúmeros problemas, desde aqueles relacionados a domínio de mercado, redução de competição e inovação, quanto a controle de discurso público. Pequenos negócios digitais não são viáveis, já que vão sendo aglutinados antes mesmo de crescerem e oferecem uma opção válida aos consumidores de serviços digitais.

O projeto de Lei admitiu a centralidade das plataformas digitais na vida cotidiana moderna, indispensável à comunicação, economia e debate público de ideias. Os legisladores reconheceram que desde 1996, quando foi aprovada a Telecommunications Act, não houve outra iniciativa de regulação do setor de comunicação e tecnologia. Com isso, as plataformas digitais ficaram livres para fazerem suas regras de autorregulação sem a devida contribuição democrática e responsabilidade (Lei). Douglas (2023) também reconhece que houve uma lacuna na regulação das plataformas digitais nos EUA, porém, nos últimos cinco anos, várias propostas têm nascido no Congresso com o intuito de tornar a política estadunidense mais intervencionista. Mas estas iniciativas, na maioria das vezes, não passam da introdução no Congresso.

O projeto aponta que a autorregulação, sem o devido monitoramento, trouxe problemas como: sufocamento de pequenos negócios; colapso da confiabilidade do jornalismo profissional; aumento de doenças mentais e comportamento adicto de usuários, especialmente menores; disseminação de desinformação; monetização de dados pessoais de cidadãos sem o seu devido consentimento; e, aumento de radicalismo e violência. Os EUA teriam perdido, nesta lacuna, a possibilidade de ditar regras, já que outros competidores globais vêm fazendo a regulação das plataformas digitais em seus territórios. Assim como, deixaram de lado seu histórico de regular grandes setores, visando a diversidade de ideias, envolvimento civil e direito dos cidadãos de se comunicarem e autogovernarem.

A FDPC teria jurisdição a qualquer plataforma digital que origina ou recebe serviços nos EUA e que afeta o comércio interestadual ou internacional. As regras deveriam ser editadas, com observação ao Code Council, com prazo máximo de 180 dias após a promulgação da Lei. Deveriam conter parâmetros técnicos e comerciais, como: portabilidade de dados; funcionalidades de sistemas operacionais (compartilhamento de dados e demais informações); recomendações para sistemas algorítmicos justos, transparentes e seguros; transparência dos termos de serviço, inclusive sobre política de moderação de conteúdo; requisitos de riscos públicos de distribuição de conteúdo nocivo e medidas sistemáticas para mitigar o problema; obrigações e transparência de divulgação de informações para a FDPC, auditorias de terceiros e pesquisadores; padrões de acesso a pessoas portadoras de deficiência.

Douglas (2023) denota que uma das maiores dificuldades na elaboração do arcabouço regulatório reside na colaboração de agências federais, que costumam

trabalhar isoladamente. O ecossistema regulatório das plataformas digitais exigiria uma mudança de estruturação das instituições para atendimento de demandas conjuntas. Por exemplo, as ações da FDPC podem facilmente sobrepor as da FTC ou da Federal Communication Commission (FCC), que fiscaliza a oferta de sinal por provedores de internet. A redundância de ação não é de todo negativa, porém, a colaboração das agências federais regulatórias demanda do Congresso um sistema de regras que compreenda obrigações estatutárias sistemáticas, com vias de efetivamente dar suporte à interconexão para fiscalização e punição de infratores. O que emerge desta ideia é um controle vertical do executivo e judiciário sobre as agências e uma influência horizontal entre elas.

5.3.3 Mecanismos legais da União Europeia

Diferente do Brasil e dos EUA que trabalham com Leis e projetos de Leis, a União Europeia tem em seu arcabouço legislativo os seguintes instrumentos: Regulamentos, Diretivas, Decisões, Recomendações e Pareceres. Regulamento é um ato legislativo vinculativo, já em estado finalizado para execução nos Estados-Membros. Diretivas normalizam um objetivo comum e os Estados-Membros devem elaborar legislações internas que sigam o parâmetro proposto. Decisões são vinculativas apenas aos Estados-Membros a elas destinados, portanto, não têm ação uniforme em todo o bloco. Recomendações permitem aos setores atingidos emitirem suas opiniões para legislações futuras. Pareceres apresentam um quadro sobre um determinado setor, não têm caráter vinculativo[47].

Devido à diferença na forma de construção da legislação da União Europeia, para atender os parâmetros estabelecidos nas dinâmicas anteriores, optou-se nesta tese por analisar apenas os Regulamentos e Diretivas. O primeiro pelo seu caráter executivo e vinculativo, uniforme a todos os Estados-Membros da UE, já o segundo pela determinação de parâmetros para a elaboração de Leis que devem harmonizar com as diretrizes estabelecidas, com legislações construídas pelos Estados-Membros. O Quadro 15 apresenta quais instrumentos legais da UE serão analisados.

[47] Tipos de Legislação. Disponível em: https://european-union.europa.eu/institutions-law-budget/law/types-legislation_pt Acessado em 03/08/2023.

Quadro 15 – Instrumentos de regulação propostos na UE 2006 a 2022

Mecanismo legal	Autor	Data	Resumo da proposta
Directiva 2010/13/UE	Comissão Europeia	10/03/2010	Trata da coordenação das disposições legislativas, regulamentares e administrativas dos Estados-Membros com respeito à oferta de serviços de comunicação social audiovisual.
Directiva 2011/92/UE	Comissão Europeia	17/12/2011	Estabelece regras mínimas relativas à definição dos crimes e sanções no domínio do abuso sexual e da exploração sexual de crianças, da pornografia infantil e do aliciamento de crianças para fins sexuais.
Regulamento (UE) 2016/679 - Regulamento Geral sobre a Proteção de Dados (RGPD)	Comissão Europeia	27/04/2016	Estabelece o regramento para tratamento dos dados de cidadãos europeus pelas plataformas digitais.
Directiva 2017/541	Comissão Europeia	15/03/2017	Trata de questões relativas à luta contra o terrorismo e que substitui decisões anteriores.
Directiva 2018/1808/UE	Comissão Europeia	14/11/2018	Atualiza a Diretiva 2010/13/UE que trata da oferta de serviços de comunicação social audiovisual para abarcar plataformas de serviço de streaming e compartilhamento de vídeos.
Diretiva (UE) 2019/790	Comissão Europeia	17/04/2019	Trata de questões relativas aos direitos de autor e direitos conexos no mercado único digital e que altera normas anteriores.
Regulamento (UE) 2019/1150	Comissão Europeia	20/06/2019	Estabelece as regras para relacionamento entre o usuário que utiliza as plataformas digitais de forma profissional para oferta de bens e serviços a usuários consumidores.
Regulamento (UE) 2021/784	Comissão Europeia	29/04/2021	Estabelece as normas relativas ao combate à difusão de conteúdos terroristas em linha e complementa Diretiva 2017/541.
Regulamento (UE) 2022/991	Comissão Europeia	08/06/2022	Estabelece o regramento para tratamento de dados pessoais para investigações policiais da Europol e trata de cooperação entre plataformas digitais e forças de segurança.
Regulamento (UE) 2022/1925 –	Comissão Europeia	14/09/2022	Estabelece regras de equidade para o mercado único digital europeu.

Regulamento dos Mercados Digitais			
Regulamento (UE) 2022/2065 – Regulamento dos Serviços Digitais	Comissão Europeia	19/10/2022	Estabelece regras para a oferta de serviços digitais no mercado comum europeu.
Diretiva (UE) 2022/2555	Comissão Europeia	14/12/2022	Cria parâmetros para a cibersegurança e faz recomendações para a formulação de legislações quanto às obrigações das plataformas digitais.

Fonte: Elaborado pela autora

Cabe a ressalva de que algumas normas são analisadas em conjunto porque um documento atualiza o anteriormente publicado, mas não necessariamente o revoga. Segundo os critérios estabelecidos, foram selecionados instrumentos legais que tratavam de moderação de conteúdo, referindo-se à liberdade de expressão, também normas com regras sobre a privacidade e segurança do usuário na rede. Para selecionar o escopo de análise utilizamos os seguintes comandos de busca no site do Parlamento Europeu: mídias sociais, redes sociais, plataformas digitais e plataformas em linha. Reforçando que as normas analisadas estavam em português.

5.3.3.1 Diretiva 2010/13UE, atualizada pela Diretiva 2018/1808/UE – Diretiva de Serviços de Comunicação Social Audiovisual

Com discussão iniciada em 2006, a Diretiva 2010/13/UE – Diretiva de Serviços de Comunicação Social Audiovisual foi proposta pela Comissão Europeia e aprovada em março de 2010, já em substituição à Diretiva 89/552/UE. O instrumento legal visava estabelecer regulamentos que seriam comuns aos países membros da UE com relação aos serviços de transmissão audiovisual. A norma primava pela garantia da "liberdade de informação, a diversidade de opiniões e o pluralismo dos meios de comunicação social" (2010, p. 1). Já em 2010 havia uma preocupação com as novas tecnologias e formas de transmissão do conteúdo audiovisual que não se restringia à programação televisiva, porém, o que a evolução tecnológica proporcionou nos anos seguintes exigiu que a norma fosse atualizada em 2018 (Otero, 2019).

A convergência dos serviços de televisão junto com a internet fez necessária a atualização do regramento de transmissão via Diretiva 2018/1808. Um dos apontamentos presentes no documento foi a visualização de conteúdo audiovisual nos

aparelhos de comunicação móvel, principalmente pela juventude. A consolidação dos serviços de *streaming* e compartilhamento de vídeos estabeleceu a necessidade de novos regramentos para o setor (Otero, 2019). De acordo com o texto, a norma teria o objetivo de trazer equilíbrio entre acesso, proteção dos consumidores e competitividade no setor.

O que fica claro na Diretiva 2018/1808 é que ela se aplica a conteúdo compartilhado em ambientes privados, como serviços de *streaming*, e em comunidades de interesse não comercial, como as plataformas de compartilhamento de vídeos, caso das redes sociais e dos app de comunicação instantânea. Todo o restante do conteúdo ainda estaria abrangido pela Diretiva 2010/13/UE. Caberia ao Grupo de Reguladores Europeus dos Serviços de Comunicação Social Audiovisual (ERGA) a avaliação em caso de controvérsia sobre a aplicação de uma norma ou da outra, quando houvesse dúvida sobre qual regra um conteúdo audiovisual tivesse que responder.

Nesta tese, foca-se a análise sobre as regras para o compartilhamento de vídeos, que são produzidos principalmente pelos cidadãos comuns e não teriam influência editorial das grandes corporações de mídia, porém, passam pelo escrutínio das políticas de moderação das plataformas digitais. A norma prevê a restrição à liberdade de prestação do serviço, em caso de ação de proteção ao consumidor, que não fosse abrangida pela Diretiva 2010/13/EU. Otero (2019) sinaliza que a convergência dos meios de comunicação tornou as plataformas digitais em centros de distribuição de conteúdo e venda de serviços e produtos. Portanto, a norma, mesmo que voltada ao conteúdo audiovisual, teria que abranger a questão consumidora, traduzida na política publicitária das plataformas, que dividem os mesmos anunciantes com os demais meios de comunicação.

O documento ressalta que a melhor forma de dirimir conflitos é por meio de autorregulação e corregulação, com apoio legislativo. Os códigos de conduta devem ser avaliados e revisados constantemente, com transparência para uma aplicação eficaz das normas. De acordo com o texto, porém, apesar da autorregulação do setor representar uma aliada complementar, ela não pode substituir os mecanismos legislativos. Estabelece-se um quadro ideal com a aplicação da corregulação, quando setor privado e o público trabalham em conjunto na elaboração de regras. Valente (2021) visualiza na normatização europeia a base, inclusive, para propostas de

legislações no Brasil, devido à forma como a UE conseguiu equalizar as demandas do setor, com o avanço tecnológico.

Como um dos pilares da democracia centra-se na liberdade de expressão, o documento ressalta a necessidade de transparência no controle das corporações de comunicação social e escrutínio sobre a propriedade das empresas ao público. Devido à influência sobre a opinião pública, os cidadãos têm o direito de saber quem são os fornecedores dos serviços de informação. Por isso, são exigidos dos operadores das plataformas informações essenciais como o nome do proprietário, endereço da empresa e site da corporação em sua instalação no território europeu.

As plataformas de compartilhamento de vídeos estão sujeitas à aplicação da Diretiva 2018/1808/UE independentemente da localização geográfica de suas sedes ou afiliadas. Práticas enganosas e agressivas em anúncios são vedadas, assim como conteúdo nocivo, discurso de ódio e utilização de dados pessoais de menores para tratamento comercial. É proibida a propaganda de tabaco e cigarros eletrônicos, nestes ambientes. Jogos de azar também não devem ser promovidos entre o público menor de idade. Normas de autorregulação e corregulação são incentivadas com relação a anúncios de produtos alimentícios com alto teor de sal, açúcar, gorduras e álcool, principalmente pelo impacto que causam em crianças e adolescentes.

Mesmo reconhecendo que as plataformas de compartilhamento de vídeo não seriam responsáveis editoriais pelo conteúdo postado em seus ambientes digitais, o texto assente que a organização e disponibilização dos materiais são ações das empresas e por isso elas devem ter mecanismos que evitem o contato de menor com conteúdo nocivo ao seu desenvolvimento físico, mental e moral, como pornografia e violência. Além disso, estabelece a necessidade de encontrar formas para verificar idade do usuário e controle parental para menores. Valente (2021) destaca que a criação de regulamentação para o conteúdo audiovisual online equaliza direitos e deveres das plataformas digitais com os demais meios de comunicação, criando uma forma de responsabilização que já existe no mercado audiovisual.

O documento incentiva as plataformas de compartilhamento de vídeos a encontrar meios para que os usuários possam categorizar seus materiais, abrindo a possibilidade de estabelecer uma classificação etária para o conteúdo. Além disso, caberia às plataformas encontrar medidas eficazes de evitar a veiculação de conteúdo que incentive agressão contra grupos minoritários. O documento desencoraja a busca ativa de conteúdo ilegal pelas plataformas digitais, mas informa que ações

governamentais podem ser feitas neste sentido. As empresas são estimuladas a criar e veicular campanhas de literacia midiática para maior conscientização do público no consumo de conteúdo audiovisual.

Segundo a norma, devem ser equilibrados os direitos fundamentais à liberdade de expressão e de informação, assim como pluralismo dos meios de comunicação, quando da moderação de conteúdo de incitamento ao ódio, à violência e ao terrorismo. Os Estados-Membros poderão criar entidades reguladoras, independentemente do Comitê de Contato, já existente no âmbito da UE. Regras mais pormenorizadas poderão ser criadas em âmbitos locais. Organismos de recursos devem ser instituídos de forma independente às partes envolvidas, para garantia de equidade nas decisões. A aplicação das normas fica a cargo do ERGA, que fica responsável pela aplicação de sanções de acordo com as irregularidades cometidas, que podem ser agravadas em caso de reincidência.

5.3.3.2 Diretiva 2011/92/EU

A Diretiva 2011/92/UE foi proposta pela Comissão Europeia e publicada em 2011. A norma trata da luta contra o abuso sexual e a exploração sexual de crianças e a pornografia infantil. O novo regramento substituiu a Decisão-Quadro 2004/68/JAI e levou em consideração toda a evolução tecnológica que tornou ainda maior o desafio de combate à pornografia infantil, que conta com ambiente digital para a propagação de imagens. São três as dimensões tratadas na norma que incluem a repressão aos autores deste tipo de crime, proteção das vítimas e prevenção do fenômeno.

Pela Diretiva 2011/92/UE são consideradas formas de abuso e exploração sexual as práticas de aliciamento de menores por meio digital, em redes sociais e salas de bate-papo online. Além de penas privativas de liberdade, os Estados-Membros são encorajados a criarem punições financeiras, sempre que a atividade de abuso e exploração sexual de menores envolver aferição de lucro. Também foi criminalizado a posse de material pornográfico; acesso intencional a sítio da *web* sabidamente utilizado para propagação de imagens de abuso e exploração sexual infantil; produção, oferta, distribuição e difusão de material com este tema.

No caso de crimes de abuso e exploração sexual praticados utilizando a internet, não é necessário haver denúncia para o procedimento de investigação. Estão previstos o monitoramento de ligações e comportamento digital para investigação, até

mesmo com utilização de identidade falsa pelos agentes policiais. Ballesteros (2023) afirma que esta é uma das iniciativas da UE para combater a exploração sexual de menores que compreende ações como território comum, no caso com financiamento de um laboratório da Europol, que dê condições de investigação em território comum, com financiamento para que os equipamentos sejam atualizados conforme a evolução tecnológica impõe.

A celebração de tratados e acordos bilaterais são incentivados para que membros da UE que tiverem feito turismo sexual infantil possam ser punidos. Empresas que promovam o turismo sexual infantil fora da UE devem sofrer regulação dos Estados-Membros. Denúncias poderão ser feitas por canais telefônicos com o início 116 na Europa. A proteção de dados, referente às informações de investigação, deverá respeitar a limitação de acordo com princípios constitucionais, que dá visualização apenas a envolvidos no processo investigatório e judicial. De acordo com Ballesteros (2023) a abordagem da UE precisa, de fato, compreender as ameaças vindas do mundo virtual e aquelas que se concretizam no real.

Zhu (2021) observa que há uma questão não discutida na Diretiva 2011/92/UE, que é a idade mínima na qual o indivíduo está capacitado para consentir a atividade sexual. Isso porque a Diretiva 2011/92/UE deixa esta questão em aberto para os Estados-Membros. O que ocorre é que esta idade varia muito de país para país e é modificada ao longo do tempo também, enquanto em 2004 a idade média para o consentimento sexual variava entre 12 e 17 anos, em 12 países europeus; em 2016 subiu para a faixa de 15 a 18 anos. Neste sentido, o que pode ser considerado pornografia nas plataformas digitais, muda significativamente e a Diretiva 2011/92/EU não foi atualizada desde a sua criação.

Apesar desta ressalva, outras questões são bem apontadas pela norma como o fato de imagens de pornografia infantil não serem considerados como itens de liberdade de expressão e opinião. A Diretiva 2011/92/EU indica que as plataformas digitais devem dificultar o seu *upload* na rede. Conteúdo desta natureza deve ser suprimido e os culpados pela propagação punidos. A Diretiva 2011/92/UE incentiva ações de cooperação entre os Estados-Membros e países fora do bloco no combate a este crime. São ainda incentivadas as ações voluntárias do setor tecnológico no enfrentamento à pornografia, abuso e exploração sexual infantil, como bloqueio de conteúdo.

5.3.3.3 Regulamento (UE) 2016/679 – Regulamento Geral de Proteção de Dados (RGPD)

O Regulamento (UE) 2016/679, conhecido como Regulamento Geral de Proteção de Dados (RGPD) foi proposto pela Comissão Europeia, publicado em 2016 e reconhece os dados pessoais como direito fundamental. Os princípios que regem o RGPD são liberdade, segurança e justiça. A norma tem o objetivo de harmonizar os direitos fundamentais dos cidadãos com a evolução econômica e desenvolvimento social, porém, o documento ressalta que o regramento foi concebido para servir às pessoas. O RGPD não entende a proteção de dados como direito absoluto, portanto ela deve ser considerada levando-se em conta a proporcionalidade, já que em alguns casos como:

> para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública, e de livre circulação desses dados, é objeto de um ato jurídico da União específico. O presente regulamento não deverá, por isso, ser aplicável às atividades de tratamento para esses efeitos. (2016, JO L 119/4, p. 4)

De acordo com o RGPD a proteção de dados precisa ser feita para que os cidadãos tenham segurança no desenvolvimento da economia digital, cada vez mais baseada nas informações fornecidas pelos usuários das TICs. E, ainda, necessita ser uniformizada na UE para garantir um exercício homogêneo no território comum de funções de interesse público ou o exercício da autoridade pública. O regramento é voltado apenas às pessoas físicas e não às pessoas jurídicas, sendo indiferente à forma de tratamento das informações se automatizada ou manual, e, ainda independentemente do local de execução da ação, se dentro ou fora do território europeu. O Regulamento abrange todo e qualquer tratamento referente à oferta de produto e/ou serviço, ou controle de comportamento no território europeu.

Quando o responsável ou subcontratante pelo tratamento de dados estiverem fora do território europeu deverão manter representante legal na Europa para responder juridicamente. A transferência de dados para outros países fora do bloco europeu fica condicionada ao respeito às normas impostas pelo RGPD. Acordos internacionais entre Estados-Membros e países de fora do bloco ou organizações estrangeiras podem ser feitos para transferência de dados, desde que todo o regramento previsto seja respeitado. A adesão à Convenção do Conselho da Europa para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados

de Caráter Pessoal será levada em consideração. Caso seja avaliado que a nação estrangeira não oferece condições de segurança razoável de dados, deverá ser proibida a transferência.

Em relação às definições dos termos, o RGPD e a LGPD (Lei Nº 13.7096, 2018)(analisada no item 5.1.3.3, p. 144 desta tese) utilizam nomenclaturas semelhantes, não sendo necessário novo quadro para pormenorização dos verbetes. Os dados identificados ou identificáveis fazem parte do escopo do RGPD, assim como os anonimizados que podem ser associados a uma pessoa por informações complementares, porém, se for impossível ou demasiadamente caro fazer a ligação entre informações e um indivíduo, estes dados ficarão fora deste regramento. Assim como estão fora do Regulamento os dados de pessoas falecidas.

Todo tratamento de dados precisa de consentimento expresso de quem sofre a ação, com descrição da finalidade específica para utilização das informações. Não é aceito pelo RGPD o consentimento tácito, portanto, é necessário que a concordância seja registrada por formulário eletrônico, ou qualquer outro meio que o responsável considerar eficiente para confirmação do registro. Quando os dados forem utilizados para múltiplas funções, todas deverão estar descritas de forma clara e concisa. No caso de investigação científica, nem sempre é possível determinar a finalidade na coleta dos dados, portanto, é preciso prever para quais finalidades o titular autoriza o tratamento, ou se ele autoriza a ação, mediante os parâmetros éticos para o estudo. Van Dijck (2022) acredita que deveria haver uma forma de tornar os dados intercambiáveis para utilizações públicas, como pesquisas em saúde, por exemplo.

No caso de menores de 16 anos, a autorização parental é obrigatória, a exceção se aplica apenas a serviços de aconselhamento e preventivo ofertados diretamente à criança ou adolescente. A licitude, equidade e transparência no tratamento dos dados são requisitos essenciais para o tratamento, apontados pelo RGPD. Portanto, os comunicados ao titular dos dados precisam ser feitos com linguagem clara, concisa e objetiva. Os contratos não podem conter cláusulas abusivas e o titular pode retirar seu consentimento a qualquer momento. O responsável pela ação ou subcontratante deve estar identificado, da mesma forma que as regras e garantias para o tratamento. A determinação de limitação de coleta e tempo de armazenagem de dados são obrigatórios. O titular deve ter real possibilidade de escolha de tratamento, correção dos dados, apagamento e portabilidade das

informações, assim como da segurança e confidencialidade, sem previsão de compartilhamento dos dados com terceiros não autorizados.

O que se observa é que em algumas áreas a preocupação com vigilância é maior do que em outras. De acordo com Martins (2019), um ano após a entrada em vigor do RGPD na Europa, o setor de telemarketing, promoções via e-mail e vídeos por demanda já haviam recebido quase 150 mil reclamações por invasão de privacidade. As pessoas queriam saber quais eram seus direitos nestas três áreas, segundo o RGPD que elas pudessem aplicar. Viola (2019) observa que a acomodação das normas leva tempo, porém, a existência delas é o que faz as empresas desenvolverem seus parâmetros de conduta e com o tempo as plataformas colocam as regras em prática.

As solicitações de informações do titular ao responsável devem ter prazo máximo de 30 dias para resposta. O titular precisa ter este direito de informação preservado, inclusive, para checagem se seus dados estão sendo tratados de acordo com a finalidade especificada em contrato. Em caso de tratamento ulterior com finalidade diferente da autorização dada, o titular deverá ser comunicado, com possibilidade de se opor à nova ação. Dados sensíveis como raça, etnia e biometria não devem ser tratados, salvo por consentimento expresso do titular, autorização judicial ou para cumprimento de direitos específicos. Esta mesma condição se aplica aos dados referentes à saúde, no que tange o interesse público para controle de epidemias, catástrofes e outras condições extraordinárias.

De acordo com o RGPD, a definição de perfis, baseado em dados com efeitos discriminatórios em razão de raça, etnia, opinião política, religião ou convicções, filiação sindical, estado genético, saúde ou orientação sexual deverá ser estabelecida pelo Comitê Europeu para a Proteção de Dados (CEPD), criado pelo regulamento. O Comitê precisa levar em conta risco para os direitos e as liberdades individuais, com possibilidade de gerar qualquer tipo de dano à pessoa natural. Riscos de dano devem ser apontados, com detalhamento sobre medidas mitigatórias, que devem ser cumpridas pelos operadores. Os parâmetros são necessários para execução das atividades de controle e fiscalização, que são exercidas por meio da conferência de relatórios com registro da atividade do responsável ou subcontratado.

Finkelstein e Finkesltein (2019) pontuam que etnia, religião, ideologia política, filiação a entidade sindical ou de outra natureza, filosofia de vida fazem parte do modo de pensar dos indivíduos. Estas questões não podem estar abertas à possibilidade de

manipulação. A garantia da segurança dos dados é uma obrigação a ser cumprida pelo responsável ou subcontratante, que também deve assegurar sigilo e confidencialidade.

Técnicas de anonimização e cifragem dos dados são recomendadas, assim como processos de testagem de eficiência de integridade das informações. Os responsáveis e subcontratantes podem elaborar códigos de conduta que respeitem os requisitos do RGPD, ou então, utilizar selos e certificações reconhecidos pelo CEPD. Quando uma violação de segurança ocorrer, o responsável ou subcontratante tem prazo de 72 horas para avisar a autoridade de controle e fiscalização sobre a exposição de dados.

A ausência de comunicação do fato só será aceita se o vazamento de informações for comprovadamente não prejudicial, apresentado pelo operador por meio de justificativa documentada. O titular também deverá ser comunicado de vazamento de informações, para ter tempo de atenuar os riscos da exposição dos dados. Sempre que um operador for dar início a uma atividade de tratamento com alto risco de salvaguardar as informações, deverá comunicar a autoridade de controle, com apresentação de medidas mitigatórias. A criação de procedimentos de certificação e selos de proteção de dados é estimulada.

Se alguém for prejudicado por ação de tratamento de dado que violou norma do RGPD, cabe ao responsável a indenização pelo dano. Além do pagamento de possíveis indenizações, os responsáveis poderão receber sanções e repreensões, como multas, que assegurem o cumprimento das normas. A gradação das penalidades dependerá da gravidade das infrações e período pelo qual foram mantidas as irregularidades. Sêmola e Blum (2021) apontam que o regramento europeu previu que a segurança dos dados deve ser feita por um time multidisciplinar, com representantes do direito, TI, psicologia, educação, monitores, todos focados num bem comum, a proteção dos dados dentro das grandes empresas.

A liberdade de expressão e de informação, no âmbito de atividade jornalística, acadêmica, artística e/ou literária deverá ser conciliada entre o RGPD e os Estados-Membros. O acesso do público a documentos em poder das autoridades estatais deverá ser considerado em comunhão com o direito à privacidade dos dados pessoais. Mesma consideração deve ser feita para dados previstos para arquivo, estudos históricos e estatísticos.

Apesar de aprovado desde 2016, o RGPD entrou em vigor em 2018. Em 2020, a Comissão Europeia apresentou um relatório ao Parlamento Europeu sobre o Regulamento. Neste relatório, a Comissão apresentou o resultado da aplicação do relatório e algumas evoluções possíveis para melhoria do ecossistema digital. A proposta é de um mercado único de dados na Europa, com separação de 10 subáreas, para desenvolvimento econômico do bloco. O documento cita o Brasil, como um dos países que a partir do RGPD também foi despertado a promover a segurança e privacidade dos dados de seus cidadãos, que é uma marca das sociedades democráticas contemporâneas. Segundo o documento, a proteção de dados proporcionada pelo RGPD também é fundamental para evitar a manipulação das decisões dos cidadãos europeus, por meio dos algoritmos de afiliação (União Europeia, 2019).

De acordo com o relatório, o Comitê tinha adotado 67 documentos, incluindo 10 novas orientações e diretrizes, e 43 pareceres, isso até o fim de 2019. Luxemburgo e Irlanda tiveram aumento de pessoal em suas autoridades de controle, já que empresas multinacionais de tecnologia se instalaram em seus territórios e estas localidades foram incumbidas das atividades de controle do tratamento de dados destas companhias. A aplicação de multas e advertências têm financiado o serviço de controle. O relatório aponta a necessidade de orientar as pessoas sobre a proteção de seus dados. Uma pesquisa apresentada no documento demonstra que 69% dos menores de 16 anos e 71% da população da UE sabem da existência do RGPD. A portabilidade dos dados é um direito ainda pouco exercido pelos cidadãos (União Europeia, 2019).

O relatório elabora um quadro de ações que deveriam ser desenvolvidas nos anos seguintes. As principais ações foram no sentido de trabalhar legislações dos Estados-Membros para assegurar o tráfego de dados no território europeu; no âmbito da Comissão Europeia tratar de maior intercâmbio de informações e propostas de alterações para aprimoramento do RGPD; para o Comitê, seguir aplicando as normas e sanções harmonizadas com as autoridades de controle dos Estados-Membros; equalizar junto aos Estados-Membros legislações que sustentem a segurança e privacidade de dados em conjunto com a liberdade de expressão (União Europeia, 2019).

5.3.3.4 Diretiva 2017/541 e Regulamento (UE) 2021/784

A Diretiva 2017/541 foi proposta pela Comissão Europeia e publicada em 2017. O documento trata do regramento referente ao combate ao terrorismo e substitui a Decisão-Quadro 2002/475/JAI do Conselho e altera a Decisão 2005/671/JAI. O documento estabelece que deve haver harmonização às Leis dos Estados-Membros para punição de atos terroristas, inclusive quando praticados com a utilização das plataformas digitais. Como pondera Ramos (2023) as duas iniciativas fazem parte de uma ação da UE baseada em um tripé, garantir a segurança dos cidadãos europeus; prevenir a radicalização primando pelos valores do território comum; e, cooperar com organismos internacionais para evitar ações não só na UE, mas em outras partes do mundo.

Foram criminalizadas práticas de treinamento para consecução de atos terroristas com acesso a material postado na internet, assim como o *upload* de manual contendo instruções para fabricar artefatos explosivos ou de treinamento para execução de ato terrorista. E, ainda, ações de radicalização e recrutamento de indivíduos para atos terroristas via plataformas digitais. Neste sentido, a distribuição ou a difusão de material público de glorificação ou justificação dos atos terroristas são puníveis em ações penais.

As plataformas digitais são incentivadas a bloquear conteúdo com incitamento público à prática terrorista. Assim como, Estados-Membros devem promover acordos com países estrangeiros para agirem no sentido de bloquearem tais sítios na *web*, que estiverem fora do território europeu. Quando esta ação de supressão na origem não for possível, o acesso ao conteúdo no território europeu deve ser promovido. A indústria digital também é incentivada a promover ações voluntárias de combate ao terrorismo online, com mecanismos de detecção e sinalização de conteúdo desta natureza, porém, as plataformas não são obrigadas a executar serviço de fiscalização e vigilância, nem podem ser consideradas responsáveis por tais materiais.

A partir de 2020, a UE focou ainda mais esforços no combate à radicalização online por conta da facilitação na comunicação transfronteiriça, que facilitava a ação de grupos radicais que não estavam na UE, mas poderiam praticar ações terroristas dentro do território comum (Ramos, 2023). Por isso, no Regulamento (UE) 2021/784 a legislação é voltada para conteúdo terrorista na *web* e traz uma série de obrigações às plataformas digitais. O documento tem início com a necessidade de equalizar a

liberdade de expressão, segurança jurídica das plataformas digitais e o combate ao terrorismo.

O Regulamento (UE) 2021/784 chama a atenção para a necessidade de um trabalho conjunto entre governos e plataformas no combate a este mal. Apesar de não serem responsáveis pelo conteúdo de terceiros, as plataformas digitais precisam estar atentas ao fato de que são ambientes vêm sendo usados para práticas ilegais, inclusive de incitação, propagação e recrutamento para práticas terroristas. A norma aponta que o conteúdo terrorista nas redes tem sido um catalisador de radicalização.

Para garantir uma uniformização de aplicação da norma, foi estabelecido que conteúdo de propaganda terrorista seria todo material que induza à prática, participação em infração, ou grupo, atividades que glorifiquem atos terroristas, por meio da difusão de *posts* que representem ações neste sentido. Também são incluídos neste item manuais de instruções sobre confecção ou utilização de explosivos, armas de fogo ou substâncias perigosas (químicas, biológicas, radiológicas ou nucleares). O conteúdo pode ser de imagens, vídeos, áudios, assim como transmissões de tais atos, gerando um exemplo que põe em risco a sociedade. A avaliação do material deve ser feita por parte da plataforma digital e das autoridades europeias, levando-se em conta a origem do material e o risco imediato aos cidadãos europeus.

O conceito de distribuição pública deste tipo de informação deverá ser considerado como de acesso a um número ilimitado de pessoas. Estão listadas nesta categoria as plataformas de mídias sociais, de compartilhamento de vídeos, áudios e imagens, e, de serviços em nuvem que forneçam conteúdo a pedido. Foram excluídos, porém, os serviços de e-mail, os de mensagem privada e que apenas faziam a armazenagem em nuvem. Para sofrerem a ação do Regulamento, os prestadores do serviço digital devem estar baseados em algum Estado-Membro ou, quando estrangeiro, ter o seu foco como o mercado comum europeu.

Conteúdo jornalístico, educativo, artístico ou de investigação ficam fora do escopo desta legislação. Leva-se em conta neste sentido o direito à liberdade de expressão e informação, assim como pluralismo dos meios de comunicação e liberdades das artes e ciências. O documento reforça que mesmo as opiniões polêmicas, radicais ou controversas de cunho político em temas sensíveis não podem ser consideradas como terroristas, assim como, material que trate da prevenção ao terrorismo e servem como um alerta ao público.

A remoção ou bloqueio de acesso a material deve ser comunicada ao produtor do conteúdo, com a motivação e a possibilidade de recurso. A comunicação só se exclui por orientação policial, para evitar risco a investigações. A exclusão precisa ser acompanhada de uma justificativa, com prova da motivação, para que o alvo possa fazer sua defesa. Caso o recurso seja reconhecido por análise célere do órgão competente, o material deverá ser restabelecido. Em caso de supressão de conteúdo feito por ferramentas das próprias plataformas, as autoridades responsáveis deverão ser comunicadas com informações sobre a localização do autor de material que ofereça risco à vida.

Após uma comunicação de que o material deve ser removido, os prestadores de serviço digital têm uma hora para a retirada do ar do conteúdo. Quando os casos não forem urgentes, os procedimentos antes da publicação devem ser comunicados às plataformas com 12 horas de antecedência, porém, apenas nos casos em que não houver risco à vida, ou grave ameaça física a pessoas. Um ponto de contato, com funcionamento de 24 horas, sete dias por semana, deve ser mantido entre autoridades e plataformas digitais para comunicação sobre material terrorista.

Os prestadores de serviços digitais podem estabelecer seus próprios termos de combate ao terrorismo. Para isso, devem manter as regras de forma clara em ambiente público para seus usuários. As ações previstas precisam ser transparentes, proporcionais e não discriminatórias. O documento aponta a necessidade de implementar medidas de sinalização e denúncia de conteúdo terrorista nas plataformas digitais, seja por meio de IA ou manual, porém, com condições de verificação das informações para evitar exclusão injustificada.

Os elementos de prova, como ID do assinante, dados de entrada e saída do ambiente digital, devem ser mantidos pelas plataformas digitais por seis meses, ou em caso de pedido de prorrogação, pelo tempo necessário à apuração do fato. A manutenção dos materiais é necessária, inclusive, para restabelecimento de conteúdo em caso de recurso administrativo ou judicial favorável, que implique a reposição do conteúdo. Os dados também poderão ser requeridos por autoridades policiais para investigação e posterior julgamento. As plataformas digitais devem estabelecer um representante legal para tratar deste assunto.

Relatórios de transparência devem ser feitos anualmente pelas plataformas digitais com suas ações de identificação e remoção de conteúdo terrorista. Também cabe às autoridades responsáveis a publicação de relatórios com suas ações. Tais

relatórios serão avaliados em 2024, para determinação de cumprimento dos princípios de eficiência, necessidade, eficácia, proporcionalidade, pertinência, coerência e valor adicionado à UE. A Comissão deverá avaliar os interesses atingidos, como liberdade de expressão, pluralismo de ideias, privacidade e proteção dos dados pessoais.

5.3.3.5 Diretiva 2019/790

A Diretiva 2019/790, publicada em abril de 2019, estabeleceu os parâmetros para o tratamento sobre os direitos autorais no mercado digital. A Diretiva entra no escopo desta tese pelo fato de tratar da responsabilidade das plataformas digitais quanto à harmonização entre a liberdade de expressão e o respeito aos direitos de autor. O texto do documento faz uma diferenciação entre divulgação de materiais protegidos para pesquisa científica, em atividades de caráter educativo ou cultural sem caráter comercial e quando na partilha de conteúdo entre usuários nas plataformas digitais, com fins lucrativos.

O documento reconhece que a utilização de material de imprensa, por usuários individuais, com divulgação de conteúdo via hiperlink não é protegida pelo direito de autor, assim como reprodução de pequenos trechos de produção de imprensa. Mas materiais protegidos pelo direito de autor devem ser remunerados quando utilizados em material jornalístico, com ganho editorial.

As plataformas digitais devem obter autorização de autores de materiais protegidos, para disponibilizá-los em seus ambientes. Quando houver um contrato celebrado entre a plataforma e os autores, a licença se estende aos usuários, caso de músicas, por exemplo. A Diretiva reconhece a responsabilidade das plataformas digitais quando um material protegido, sem acordo de utilização, é utilizado em seu ambiente digital. Cabe uma exceção à responsabilização sempre que a plataforma demonstrar que fez os esforços para obter autorização ou efetuou esforços para deixar o material indisponível em caso de comunicação efetiva e fundamentada sobre a disponibilização irregular. Os serviços de partilha de conteúdo devem dispor de mecanismos que impeçam o carregamento de material protegido.

Os usuários podem invocar direitos referentes à utilização das obras protegidas para citações, críticas, análises, caricaturas e paródias. As plataformas digitais devem ter sistemas de denúncias para direitos autorais, assim como de recursos para quem teve conteúdo bloqueado ou removido, com base nesta norma. Os titulares de direitos

autorais que denunciarem utilização indevida de material devem fornecer dados que comprovem a reclamação. Os Estados-Membros são estimulados a criarem mecanismos de recursos extrajudiciais que solucionem litígios referentes a esta questão. O direito de autor deve constar dos termos de uso das plataformas que permitem compartilhamento de conteúdo.

Geiger (2022) fez uma dura crítica à Diretiva 2019/790 afirmando que as exceções previstas pela norma para mineração de dados e utilização de obras com proteção de autor não abrangem uma disposição da própria UE de criar um ambiente de inovação. Para o autor, a utilização de material protegido para pesquisa só abarcou universidades públicas. A norma deixou de fora iniciativas como as público-privadas, em que governos se unem a empresas na busca de soluções para problemas da sociedade, que são tão incentivadas dentro do bloco, e até mesmo das *startups* que estão na base do desenvolvimento tecnológico da UE. Neste sentido, a norma fere o direito à pesquisa.

5.3.3.5 Regulamento (UE) 2019/1150

O Regulamento (UE) 2019/1150, publicado em junho de 2019, trouxe o regramento para tratar do relacionamento entre o usuário profissional das plataformas digitais e as empresas. Segundo o texto, o objetivo do documento é que o produtor de conteúdo ou fornecedor de produto ou serviço digital seja tratado de forma equitativa e transparente pelas plataformas. As normas referem-se aos serviços de intermediação digital e os motores de busca. Estão incluídos neste ecossistema as plataformas de mídias sociais, lojas de app, comparadores de preços, sites de buscas e *marketplaces*[48]. As negociações são feitas entre os usuários das plataformas digitais, que funcionam como intermediadoras das transações entre usuários fornecedores e usuários consumidores.

Para que o usuário consumidor seja protegido neste tipo de negociação, o Regulamento apresenta as obrigações para as plataformas digitais que ofertam o ambiente de intermediação das transações comerciais. Segundo o texto, as plataformas devem ter em seus termos de serviço regras claras e objetivas aos usuários fornecedores; com definição das cláusulas de cessação ou interrupção do

[48] Marketplaces são sites que reúnem vendedores de todos os tipos de produtos e serviços, como um shopping center virtual.

serviço; aviso de 15 dias para mudanças nos contratos de serviço, a exceção se aplica a casos de cibersegurança; agir de boa-fé, sem imposição de cláusulas a posteriori; explicitar quais são os direitos de autor; a cessação dos serviços deve ser fundamentada e apresentada com 30 dias de antecedência; assegurar a identificação dos usuários profissionais.

Tanto usuários fornecedores quanto consumidores precisam estar informados sobre a coleta, tratamento e armazenamentos de dados pessoais gerados a partir da intermediação de transações comerciais no ambiente da plataforma digital. A descrição dos termos deve ter categoria de dados coletados; com quem as informações poderão ser compartilhadas e a finalidade para que os dados sejam compartilhados. Segundo Viola (2019), com a existência de parâmetros os cidadãos europeus desenvolvem uma mesma experiência de compra, independentemente do local em que estejam. Isso gera conforto ao cidadão e previsibilidade para as empresas, o que é uma condição essencial para o desenvolvimento dos negócios.

As cláusulas contratuais gerais das plataformas digitais devem estabelecer regras de remuneração e no caso dos motores de busca, como é feita a classificação dos materiais; tratamentos diferenciados devem ser descritos de forma clara e objetiva; também são necessárias as descrições técnicas para a oferta do produto ou serviço digital; bem como as restrições a que podem estar sujeitos os produtores de conteúdo ou usuários fornecedores em questões infra estruturais da plataforma; e, ainda, como funcionam os sistemas de reclamação e recursos dentro do ecossistema digital. Serranía e Abrusio (2021) destacam que micro, pequenas e médias empresas são dependentes das plataformas. Esta relação desigual expunha as empresas a risco de inviabilização de negócios por imposições ou remuneração injusta das plataformas. A norma trouxe maior segurança jurídica neste sentido.

As plataformas que empreguem mais de 50 pessoas e tenham faturamento acima de €$ 10 milhões devem dispor de um setor para resolução de conflitos entre usuário, fornecedor e a empresa. Estes órgãos devem tratar de questões referentes à legislação, dificuldades tecnológicas, práticas adotadas que afetem os usuários fornecedores. Todos os procedimentos devem gerar um relatório, com acesso público, via Observatório da Economia das Plataformas em Linha, para a verificação de estatísticas sobre a solução de problemas. A solução de litígios pode ser feita por mediadores que devem ser indicados pelas plataformas digitais, com ao menos duas opções. Cada Estado-Membro deverá assegurar o cumprimento do Regulamento.

5.3.3.6 Regulamento (UE) 2022/991

Publicado em junho de 2022, o Regulamento (UE) 2022/991, estabeleceu todo o regramento para tratamento de dados pessoais dos cidadãos europeus e residentes no bloco, para as investigações policiais da Europol. Com relação às plataformas digitais, o instrumento legal cria obrigações de cooperação das empresas com as forças de segurança. Segundo o documento, em situações de crise, a Europol pode receber dados pessoais de usuários diretamente das plataformas digitais. As situações de crise são definidas como anteriores, durante ou pós incidentes reais, em situações de atentados terroristas ou ameaças que oferecem risco iminente à vida.

Para Ruiz Díaz (2022) houve um avanço nas atribuições da Europol após a instituição do Regulamento (UE) 2022/991 porque a norma garantiu uma maior capacidade de processamentos de dados dos cidadãos, com a supervisão da Autoridade Europeia para a Proteção de Dados (AEPD). A busca por maior segurança acaba por esbarrar na privacidade do cidadão e na possibilidade de abuso do poder público. As organizações da sociedade civil são claramente contrárias a estes avanços, principalmente aos acordos internacionais de cooperação. As entidades verificam que nestes momentos há um maior risco de avanço do poder de polícia, devido à troca de informações com agências de segurança internacionais que não têm a obrigação de obediência à norma europeia.

Nestes casos de terrorismo, quando Estados-Membros devem pedir o bloqueio de conteúdo viral às plataformas digitais, a Europol presta apoio na sinalização dos materiais com base no Regulamento (UE) 2021/784 (descrito no item 5.3.3.4). Também cabe à Europol a troca de informações e transferência de dados pessoais com países estrangeiros no sentido de bloqueio de endereços na *web* que estejam alojados fora do território europeu. Esta troca de informações só é prevista em casos de combate ao terrorismo e aos crimes sexuais contra menores na internet.

O enfrentamento à pedofilia e pornografia infantil estão no escopo da Lei, prevendo que a Europol pode receber informações de empresas para combate a estes crimes. O intercâmbio de informações pode ser feito também no sentido oposto da Europol para as plataformas digitais, por meio de requisições de bloqueio e identificação de suspeitos na propagação de conteúdo desta natureza. As requisições de informações devem ser feitas aos representantes legais das empresas em território

europeu, com máximo detalhamento sobre a causa do pedido e limitados à investigação para o combate aos crimes previstos.

A Europol pode sinalizar, junto às plataformas digitais, os materiais ilegais para que sejam analisados voluntariamente pelas empresas, com base em seus próprios termos de serviço. Também deve ser facultado às plataformas digitais a entrega opcional de relatório sobre conteúdo moderado, potencialmente ilegal para que a Europol proceda a investigação. Em todos os casos anteriormente descritos, os direitos e liberdades individuais não sobrepõem os direitos públicos.

5.3.3.7 Regulamento (UE) 2022/1925 – Regulamento dos Mercados Digitais

O Regulamento (UE) 2022/1925 trouxe as normas de equilíbrio para o mercado único digital da Europa. Altera as Directivas (UE) 2019/1937 e 2020/1828 que indicavam aos Estados-Membros as diretrizes para formulação de instrumentos legislativos para tratar do assunto. O documento trouxe em toda a Europa a harmonização das regras para empresas, usuários profissionais e consumidores, devido à importância cada vez mais crescente da economia digital. As plataformas digitais foram consideradas essenciais e por isso, foi vedado aos Estados-Membros obrigações adicionais, com relação aos temas já previstos neste instrumento, na intenção de garantir a livre concorrência do mercado digital.

Tommasi *et al.* (2022) apontaram que menos de dois anos da proposta inicial, o Regulamento (UE) 2022/1925 foi aprovado. Este é um dos pivôs da economia pensada para o bloco europeu para os próximos anos. Os legisladores se preocuparam com o domínio que as plataformas digitais vêm tendo da economia global. Foram considerados como controladores de acesso, ou *gatekeepers* essenciais, empresas que movimentaram na Europa €$ 7,5 milhões nos três últimos anos, com 45 milhões de usuários ativos mensalmente e 10 mil usuários profissionais em exercício anualmente. Estas empresas tinham até 2 de julho de 2023 para comunicar às Comissão Europeia que faziam parte deste Regulamento.

De acordo com a norma, as plataformas digitais não podem: reutilizar dados para prestação de outros serviços, a não ser os seus essenciais; impor restrições à forma de pagamento dos seus próprios serviços; obrigar assinatura de outros serviços oferecidos; favorecer seus próprios serviços em detrimento dos de terceiros ofertados em seus ambientes digitais; a não ser que tenha recebido consentimento expresso

para tais ações. Tommasi *et al.* (2022) observam que as obrigações são proporcionais e cumulativas, dependendo do seu posicionamento de mercado. Elas foram divididas em ambientes de alojamento, plataformas online e plataformas online de grandes dimensões.

O Regulamento (UE) 2022/1925 estabelece que os *gatekeepers* não podem influenciar a forma como o produtor de conteúdo profissional oferece seus serviços ou produtos aos usuários finais das plataformas digitais. Até mesmo as formas legais de resolução de conflitos não podem ser influenciadas pelas plataformas, que também estão vetadas de obrigarem aplicativos ou navegadores aos usuários. Anúncios feitos nas plataformas digitais devem ter formas de demonstração de efetividade métrica aos publicitários. Taxas e deduções de impostos devem ser demonstradas. As plataformas não podem utilizar dados dos produtores de conteúdo, gerados a partir deles ou de terceiros, para ofertas concorrenciais. É vedado ainda sistema discriminatório de indexação de conteúdo. Para Tommasi *et al.* (2022) esta foi uma medida de previsão de equidade entre os envolvidos em serviços intermediados por plataforma digital.

Não é possível que um *gatekeeper* interfira em aplicativos baixados pelo usuário final em sua máquina. É obrigatório às plataformas digitais a interoperabilidade do sistema utilitário do serviço digital e dos softwares instalados pelo usuário em sua máquina. A portabilidade de dados foi estabelecida como mais uma exigência, assim como acesso aos dados pelo titular. Para os produtores de conteúdo e fornecedores de produtos ou serviços digitais é obrigatório acesso a dados relativos ao negócio, inclusive com apresentação de relatórios em linguagem acessível. As plataformas também não podem discriminar um produtor de conteúdo ou fornecedor de bens e serviços porque este oferece material em condições diferentes em uma outra plataforma.

A cessação de serviços por parte da plataforma não pode ter cláusulas abusivas e por parte do usuário não pode ser dificultada. É obrigatória a apresentação de condições de segurança, sigilo e criptografia de mensagens trocadas pelos usuários, assim como para armazenagem de dados. É proibido às plataformas digitais subdividir ou fragmentar a empresa para isentar-se de cumprimento das normas estabelecidas. O cumprimento do Regulamento deve ser acompanhado pela Comissão Europeia, que tem prerrogativas investigatórias e executivas de penalidade. Sanções e multas podem variar entre 10 e 20% do faturamento das empresas. A

Comissão fica autorizada a emitir atos delegados, para novas obrigações, principalmente no intuito de alargar obrigações em benefício dos usuários profissionais e finais.

5.3.3.8 Regulamento (UE) 2022/2065 – Regulamento dos Serviços Digitais

O Regulamento (UE) 2022/2065 estabeleceu as regras para oferta de bens, serviços e conteúdo digitais e ficou conhecido como Regulamento dos Serviços Digitais. O documento alterou a Diretiva (UE) 2000/31/CE que tratava principalmente do comércio eletrônico na internet. Com a evolução das transações possíveis via ciberespaço a norma estava defasada e a atualização trouxe novas obrigações tanto a plataformas digitais, quanto a fornecedores de bens e serviços online. O documento se fundamenta em três pilares: 1) a proteção dos consumidores, com respeito aos direitos fundamentais, menor exposição a conteúdo ilegal; 2) transparência e responsabilidade das plataformas digitais, com mecanismos claros de sinalização de conteúdo ilegal; 3) promoção de inovação, incentivando o desenvolvimento de plataformas iniciantes, pequenas e médias.

Como ponderam Tommasi *et al.* (2022), o Regulamento (UE) 2022/2065 foi discutido desde 2020, com mudanças que primeiro foram aceitas e depois rejeitadas em acordos políticos. Parte das normas entrou em vigor já em novembro de 2022, com referência aos grandes *players*, que são as plataformas dominantes de mercado e as demais recebendo prazo até fevereiro de 2024 para serem implementadas. O sistema conta com supervisão da Comissão Europeia, designação de coordenadores de serviços digitais em nível de Estados-Membros, e cooperação do Comitê Europeu de Serviços Digitais.

O documento reafirma a proteção do cidadão, que deverá ficar menos exposto a conteúdo ilegal e terá melhores condições para escolhas de preço. A norma trouxe ainda segurança jurídica aos prestadores de serviço, com auxílio no início e expansão de seus negócios. O Regulamento abrange empresas que oferecem a infraestrutura de rede, aqueles que fazem o alojamento de endereços virtuais, as plataformas em linha, que incluem lojas virtuais, *marketplaces*, redes sociais; e, no caso das plataformas utilizadas por pelo menos 10% dos cidadãos europeus (450 milhões de pessoas), o regramento é ainda mais severo.

O nível das obrigações depende do tamanho do negócio digital. No caso das plataformas digitais, objeto desta tese, as obrigações incluem: apresentação de relatórios de transparência; manutenção dos direitos fundamentais dos usuários; cooperação na execução de ordens das autoridades nacionais; apresentação de ponto de contato e representante legal no território europeu; prestação de informações aos usuários; notificação das infrações penais cometidas no ambiente digital; mecanismos para reclamação e recurso administrativo de litígios; sinalizadores de confiança; medidas contra notificações abusivas; verificação da idoneidade de fornecedores para proteção do mercado digital; proibição de anúncios dirigidos a crianças; transparência nos sistemas de recomendação de conteúdo, transparência dos algoritmos de publicidade e métricas da atividade.

Para as plataformas com controle de mais de 10% dos consumidores europeus soma-se ainda obrigações relacionadas à gestão de situações de crise; auditoria independente de conformidade com o regramento estabelecido e responsabilização pública; oferecimento de opção ao usuário de recusar sistema de perfilamento algorítmico; compartilhamento dos dados com autoridades nacionais e investigatórias; adoção de códigos de conduta; e, cooperação de respostas em meio a situações de crise. Orofino (2022) aponta que o Regulamento (UE) 2022/2065 busca um ambiente digital mais plural e seguro para os usuários, criando um sistema de supervisão mais eficaz das autoridades. O documento incentiva ainda um processo de autorregulação e corregulação.

Os usuários podem contestar a remoção de conteúdo e têm direito à solução de litígios em seus próprios países. Todas as condições de utilização dos serviços deverão ser previamente conhecidas pelos usuários por meio de termos claros de utilização, em linguagem acessível. A propagação viral de conteúdo ilegal ou nocivo deverá ser combatida pelas plataformas digitais, com sistemas de notificação para situações de crise envolvendo saúde ou segurança. As empresas também estão proibidas de direcionar conteúdo publicitário a menores. Estão ainda obrigadas a manterem práticas justas de negócio de forma não discriminatória. A portabilidade dos dados também deve ser uma opção prevista aos usuários. Orofino (2022) pondera, porém, que o sucesso da norma depende da participação do usuário no processo.

De acordo com levantamento feito pela Comissão Europeia, há mais de 10 mil plataformas em operação no mercado comum, sendo que 90% das empresas são consideradas de porte pequeno ou médio. Cerca de 40% do comércio europeu é feito

em plataformas digitais. Obrigações mais onerosas são inaplicáveis às micro e pequenas empresas do setor, quando ultrapassarem os limites de negócio que lhe imponham regramento mais restritivo, terão 12 meses para adaptação. As empresas deverão ter sistemas de sinalização de conteúdo ilegal, incluindo o desrespeito a material protegido por direito autoral. As plataformas têm obrigação de conhecer os fornecedores de bens e serviços, com controles de rastreabilidade das empresas, para responsabilização por comércio ilegal.

O Regulamento trouxe também segurança jurídica para as plataformas digitais, que estão sujeitas às obrigações impostas dentro deste arcabouço, não sendo possível aos Estados-Membros legislar em temas já tratados e estabelecidos neste instrumento legal. A isenção de responsabilização como intermediárias de conteúdo foi reforçada, a exceção se aplica apenas quando a plataforma tiver conhecimento do material ilegal e não tomar qualquer atitude para removê-lo. A cooperação com as autoridades depende de ordens judiciais claras e com exigências mínimas de finalidade e proporcionalidade.

5.3.3.9 Diretiva (UE) 2022/2555

Publicada já no fim de 2022, a Diretiva (UE) 2022/2555 trata dos parâmetros de cibersegurança que contempla segurança das infraestruturas dos sistemas de rede e informação, do hardware, do software e das plataformas digitais de compartilhamento de conteúdo. O documento altera o Regulamento (UE) 910/2014 e a Diretiva (UE) 2018/1972 e revoga a Diretiva (UE) 2016/1148 (Diretiva SRI 2). O Regulamento e as Diretivas que são modificadas pela Diretiva (UE) 2022/2555 tratam da infraestrutura de comunicação eletrônica e dos serviços de comunicação interpessoal, por isso não foram analisados anteriormente analisadas nesta tese, porque não ofereciam normas para plataformas de mídias sociais, que fazem parte do objeto investigação. Callejón (2022) aponta que é justamente esta a principal evolução do pensamento em cibersegurança da UE, a previsão do tratamento de ameaças advindas das plataformas de compartilhamento de conteúdo.

Além de trazer à luz a exigência de cibersegurança para as plataformas de compartilhamento de conteúdo a Diretiva (UE) 2022/2555 alertou para as dificuldades maiores para pequenas e médias empresas em manter parâmetros de confiabilidade de todas as ações online, compreendendo desde o trabalho remoto, às transações

econômicas via rede. Os ataques de *ransonware*, por exemplo, no qual os bandidos sequestram dados e informações, muitas vezes impedem o funcionamento dos sistemas operacionais e estão ficando comuns. Para as médias e pequenas empresas a diretiva indicou a necessidade de ajuda dos Estados-Membros no reforço da cibersegurança.

No geral, a Diretiva (UE) 2022/2555 indicou a necessidade de respeito às regras internacionais de cibersegurança, cartilhas de boas práticas e compartilhamento de informações para equacionamento das ameaças. As ações devem ser feitas em cooperação com a ENISA, que é a agência de Cibersegurança da União Europeia, fundada em 2004. Callejón (2022) observa que é preciso manter uma uniformidade na abordagem de cibersegurança pelos Estados-Membros para garantir uma uniformidade de tráfego de dados em áreas de fronteira. Para isso, é preciso estabelecer mecanismos de regulação, atualizando servidores e atividades sujeitas à segurança cibernética.

De acordo com a Diretiva (UE) 2022/2555, todas as plataformas digitais, que prestam serviço na Europa precisam estar harmonizadas com as normas executivas de cibersegurança propostas para empresas e usuários. O sistema DNS, por exemplo, que liga o usuário de uma máquina a um endereço na *web*, exige um grau de confiabilidade extremo, porque este recurso leva o internauta a um ambiente digital que ele mesmo solicitou via barra de navegador em seu terminal. O sistema DNS tem acesso ao IP da máquina e às informações sensíveis do usuário.

Para as plataformas digitais, a Lei a que ficam sujeitas é do Estado-Membro onde mantiver o seu estabelecimento principal na Europa, como filial, mesmo que se trate de uma empresa estrangeira. Os registros destas empresas, assim como contatos de responsáveis, deverão ser enviados à ENISA, que manterá as comunicações oficiais com os representantes legais das empresas e devem ser comunicados em caso de mudança. Cabe à ENISA auxiliar os países na elaboração do arcabouço regulatório para a cibersegurança. As sanções e multas serão aplicadas por estes Estados-Membros em caso de irregularidades.

Para Callejón (2022) o que vai garantir o cumprimento da Diretiva (UE) 2022/2555 são os dispositivos de fiscalização e a possibilidade de impor sanções tanto administrativas quanto jurídicas, com a aferição de multas. O constante controle sobre os incidentes poderão ajudar no mapeamento das ameaças cibernéticas. Com isso, novos regramentos poderão ser desenvolvidos.

5.4 Síntese de resultados de normas regulatórias de Brasil, Estados Unidos e União Europeia

Nota-se que o ordenamento jurídico brasileiro resistiu à entrada na discussão da regulação para as plataformas digitais. Mas mesmo resistente, Leis como o Marco Civil da Internet (Lei 12.965, 2014), aprovado em 2014, serviram de incentivo para a discussão sobre regulação das plataformas digitais, até mesmo em outras partes do mundo. Observa-se, porém, que a agenda regulatória nos territórios analisados toma corpo de fato a partir de 2018. Entre 20% e 30% dos instrumentos regulatórios foram discutidos antes desta data nas casas legislativas, a maior ênfase na propositura de projetos de Leis de regulação se deu a partir de 2021 e 2022. Os parlamentares estadunidenses são profícuos na apresentação de propostas, porém, lentos na aprovação das Leis. Os legisladores brasileiros seguem o exemplo estadunidense. Já as normas editadas na UE têm uma maior abrangência e efetividade, apesar de serem em menor número.

Quando observados os temas tratados neste estudo, que são a liberdade de expressão, privacidade e segurança, nota-se que todos os instrumentos regulatórios aprovados nos EUA relacionam as três dimensões, na Europa são oito normas que conjugam as temáticas e quatro do Brasil que trazem em seu bojo os assuntos relacionados. A UE tem ainda um instrumento que trata apenas de liberdade de expressão, outro que estabelece regramento sobre a privacidade do usuário e um terceiro que conjuga somente privacidade e segurança. Portanto, observa-se que as sociedades democráticas prezam pela liberdade de expressão, privacidade e segurança, de forma conjugada, já que estes são direitos fundamentais do cidadão.

Quanto aos projetos de Lei, a segurança é a temática mais presente, aparece em 33 propostas nos EUA e 13 no Brasil. Em segundo lugar estão projetos de Lei que discutem liberdade de expressão, presente em 25 proposituras nos EUA e oito no Brasil. A privacidade, de forma isolada, foi tema de um projeto de Lei brasileiro e 17 nas casas legislativas estadunidenses. Analisando, em formas conjugadas, liberdade de expressão e segurança figuraram em 10 projetos de Lei nos EUA e três no Brasil; privacidade e segurança foram observados em oito propostas de legisladores estadunidenses e duas de brasiLeiros; liberdade de expressão e privacidade contaram com uma proposta por aqui; a junção de liberdade de expressão, privacidade e segurança geraram um projeto de Lei no Brasil e outro nos EUA.

Com relação à liberdade de expressão percebe-se por parte dos legisladores uma dificuldade de estabelecimento de parâmetros objetivos para a moderação de conteúdo nas redes. Como o princípio da liberdade de expressão é basilar para as sociedades democráticas, a interferência no direito de manifestação do pensamento do cidadão pode transformar o mecanismo regulatório num instrumento de censura, o que não coaduna com a democracia. Os instrumentos legais que tratam do tema acabam partindo para a exemplificação e pormenorização das situações em que a moderação do conteúdo seria permitida, o que dificulta a aprovação das Leis. Isso porque sempre vai haver uma conduta não exemplificada e a ação das autoridades, por meio de Lei, fica inviabilizada.

Os instrumentos legais aprovados, que tratam de liberdade de expressão, geralmente propõem a moderação de conteúdo considerado ilegal. Por exemplo, a exploração sexual é crime no Brasil, EUA e UE, conteúdo desta natureza foi considerado passível de moderação com instrumentos legais já aprovados nos países e bloco econômico analisados, caso da COPPA (EUA) e Diretiva 2011/92/UE. No Brasil, a Lei Carolina Dieckmann previu punição para quem dissemina conteúdo sexual não autorizado. Esta é uma temática também bastante presente em projetos de Lei discutidos nas casas legislativas.

O terrorismo é outro tema pacificado, conteúdo desta natureza deve ser moderado, sob pena de sanções às plataformas digitais, como prevê a Diretiva 2017/541 e o Regulamento (UE) 2021/784. A moderação de conteúdo ainda trata de direito de autor, que está cada vez mais restritivo. A monetização de conteúdo digital faz com que autores sejam beneficiados com pagamento de multas, em caso de material publicado sem autorização, como prevê a Diretiva 2019/790, na UE. A materialização das Leis torna possível o requerimento de indenização por propagação de material protegido pelos direitos de autor.

Nota-se, no entanto, uma dificuldade quanto a temas que não têm uma definição estabelecida como o chamado discurso de ódio. Sem um parâmetro objetivo, os projetos de Lei seguem para exemplificações que não abrangem todo o espectro do assunto para que a moderação seja exercida sem questionamentos, por isso mesmo, não há, até o momento, instrumentos legais aprovados especificamente sobre este tema. Nos EUA, onde a 1ª emenda da constituição prevê a liberdade como cláusula pétrea, há uma profusão maior de projetos de Lei que tratem especificamente sobre o direito de manifestação do pensamento. Entre as 25 proposituras coletadas

no período de análise, nota-se uma constante criação de projetos e versões contrárias, por visões políticas antagônicas.

A aprovação de instrumentos legais tratando da moderação de conteúdo tirou das plataformas digitais a supremacia na decisão de retirada do ar de material publicado. Para Dos Santos (2020), o advento do MCI (Lei nº 12.965, 2014) no ordenamento legislativo brasileiro abriu espaço para a possibilidade de contestação jurídica das plataformas digitais, com base em um instrumento legal e não apenas conforme o que estava previsto em normas autorregulatórias das próprias empresas. A falta de instrumento legal anterior deixava o ambiente brasileiro incerto. A possibilidade de levar os conflitos ao judiciário para determinação de legalidade de material postado na internet retirou das plataformas a decisão unilateral, atentando para a letra da Lei, evitando possíveis abusos de remoção injustificada.

Com relação à privacidade do usuário, numa comparação entre as legislações Finkelstein e Finkelstein (2019) notaram que enquanto Brasil e União Europeia exigem consentimento do usuário sobre tratamento de dados pelo poder público, nos EUA é aceito o consentimento tácito. Diferentemente de Brasil e UE, não havia nos EUA, até o fim de 2022, uma Lei semelhante à LGPD (Lei Nº 13.7096, 2018)e ao RGPD. As questões de consentimento de tratamento dos dados de cidadãos estadunidenses estão espalhadas em instrumentos legais que legislam sobre questões específicas, como a COPPA (detalhada no ponto 5.3.2.3). Mas não há uma Lei que compreenda o tratamento de dados especificamente em situações diversas. É comum nos EUA que os usuários recebam apenas uma comunicação da continuidade de tratamento dos dados. Neste caso, para a interrupção de tratamento é necessária uma comunicação oficial por parte do indivíduo.

Amato *et al.* (2022) destacam que antes da LGPD (Lei nº 13.709/2018), o tratamento de dados no Brasil estava espalhado em outros instrumentos legais como o Marco Civil da Internet (Lei nº 12.965, 2014), o Código de Defesa do Consumidor e a Lei do Cadastro Positivo (Lei nº 12.414, 20111). A partir da LGPD (Lei nº 13.709/2018), o país centra seu entendimento com relação ao tratamento de dados em geral e isso inclui os serviços de internet. A LGPD (Lei Nº 13.7096, 2018)foca no acesso aos dados em território nacional, mas observando o ordenamento jurídico exterior, pela crescente pressão internacional no sentido de resguardar a privacidade dos usuários da rede (Sêmola; Blum, 2021).

Finkelstein e Finkelstein (2019) pontuam que o instrumento legal brasileiro entrou em consonância com outros instrumentos legais vigentes no exterior, como o RGPD europeu, adotando o critério da extraterritorialidade. Assim, a LGPD (Lei Nº 13.7096, 2018) determinou que “independentemente de sua origem geográfica, ao ser acessado ou acessar sistemas localizados no território nacional, deve adimplir com suas regras” (p. 296). Para Barreto Junior, Sampaio e Gallinaro (2018) é preciso aperfeiçoar a fiscalização das plataformas, porque um simples clicar numa caixinha de li e concordo não abrange o que está previsto no ordenamento jurídico, sobre as informações claras e detalhadas para a tomada de decisão. Com um mundo cada vez mais dependente dos serviços digitais, o exercício de direitos fundamentais acaba ficando em segundo plano, trocado pelo usufruto do que as plataformas oferecem.

Muitos dos artigos da LGPD (Lei Nº 13.7096, 2018)brasileira são similares, de certa forma, ao RGPD europeu. É o caso, por exemplo, do tratamento de dados de cidadãos fora do território nacional. Para que isso seja feito é preciso que o país destinatário das informações tenha as mesmas condições de segurança oferecidas no Brasil e as empresas apresentem códigos de conduta, selos e certificados de segurança. Como o Brasil tem a ANPD a UE tem a Comissão de Proteção de Dados, fixada na Irlanda, que funciona de forma semelhante. A ANPD e a Comissão devem zelar pela proteção de dados, segredos comerciais, fiscalizar e aplicar sanções, apreciar petições, promover ações de cooperação entre empresas e governos, editar regulamentos. A diferença na UE é que cada Estado-Membro também tem uma entidade de controle interno, que auxilia na aplicação das normas.

A importância da proteção dos dados pessoais no Brasil foi reconhecida, inclusive, como direito constitucional com a Emenda Constitucional nº 115/2022. O usufruto da posse dos dados com previsão de acesso e até portabilidade das informações dá ao cidadão maior autonomia de como vai usufruir deste ativo pessoal. “O titular de dados na LGPD (Lei Nº 13.7096, 2018)também significa o símbolo da igualdade jurídica na economia dos dados, pois a referida Lei trata os dados pessoais como mercadoria universalizada, disponível a todos no mercado” (Fornasier; Knebel, 2021 p. 1020). Na UE, a nova frente de discussão e busca pelo estabelecimento de um arcabouço legislativo eficiente reside na segurança dos dados e como as plataformas digitais podem garantir que as informações particulares não serão expostas. Até 2022, as determinações legais estão em diretivas e não ainda em regulamentos.

A segurança do usuário das plataformas digitais está diretamente ligada às duas dimensões anteriores, tanto a privacidade quanto a liberdade de expressão. Isso porque as plataformas digitais tratam principalmente da forma como as pessoas se relacionam na rede ou compartilham informações. A segurança nestas ações é tão importante que o tema está presente em 46 propostas legislativas, juntando Brasil e EUA. Por meio dos relacionamentos sociais, através das plataformas digitais, crianças podem ser cooptadas por criminosos para exploração sexual, indivíduos podem ser aliciados por terroristas ou quadrilhas e estes são apenas dois exemplos de como as plataformas digitais podem expor o cidadão a risco.

Transações comerciais na rede podem ser feitas com intenções criminosas como tráfico de drogas, armas e até pessoas. Outra forma de utilização das plataformas digitais para práticas criminosas é o roubo de dados para a aplicação de golpes. Como o mundo está cada vez mais digitalizado, as ações delituosas podem compreender sistemas bancários, judiciários e até eleitorais. A UE tem avançado em aprovações de mecanismos legais de proteção dos usuários, fornecedores de produtos e serviços e dos sistemas oferecidos pelas plataformas digitais.

A Diretiva (UE) 2022/2555 trata exatamente da cibersegurança de infraestrutura de rede, *softwares* e *hardwares* para minimizar os riscos de acesso a informações sigilosas dos usuários. O documento prevê parâmetros de cibersegurança mínimos às empresas e protocolos para gestão de crises, como os ataques de *ransonware*, que são os sequestros de dados, com pedido de resgate. Já o Regulamento (UE) 2022/2065 tratou do comércio eletrônico e prevê sanções para quem expor o consumidor a conteúdo ilegal, dando transparência aos usuários para bloqueio deste tipo de material. O Regulamento (UE) 2019/1150 prevê a equidade entre fornecedores e plataformas digitais, na comercialização de serviços ou produtos, trazendo previsibilidade nas transações.

Nos EUA, o projeto de Lei Stop Online Piracy Act (H.R.3261) previa a criminalização da pirataria online, com a venda de produtos de marcas protegidas falsificadas. Outro aspecto da segurança é a exposição a conteúdo impróprio ou sensível, cuja temática é contraindicada a determinadas faixas etárias, ou indivíduos sem condição de assimilação do conteúdo, pelo baixo desenvolvimento psicológico ou ainda em construção. Isso ocorre no caso de imagens explícitas de violência, sexo, consumo de substâncias psicoativas, entre outros temas sensíveis como distúrbios alimentares. Há conteúdo, porém, contraindicado a qualquer pessoa, como a

divulgação de execuções terroristas, que contempla uma das dimensões do ataque, a propagação da mensagem de intimidação do grupo extremista.

O caminho da regulação de plataformas digitais para garantia da liberdade de expressão e ao mesmo tempo possibilidade de responsabilização do usuário por conteúdo impróprio ou ilegal é longo. Assim como, está longe de haver um consenso sobre o nível de privacidade que a sociedade contemporânea deseja, em tempos de relacionamentos sociais predominantemente vividos via plataformas digitais. É necessário, porém, que existam parâmetros mínimos de segurança, para reduzir o impacto negativo num possível vazamento de dados e consequente exposição da privacidade do usuário.

5.5 Discussão e cruzamento de normas autorregulatórias com instrumentos legais

A última etapa desta pesquisa consiste na comparação entre instrumentos autorregulatórios do Twitter e normas governamentais de regulação de Brasil, Estados Unidos e União Europeia que foram aprovadas ou que passaram por discussão. Nesta etapa a tese é afirmada no sentido de que a regulação estatal cria nas plataformas digitais o movimento da autorregulação. Foi possível observar que no período de discussão, os projetos de Lei eram utilizados como base pelas plataformas digitais para elaborar suas próprias regras.

A comparação foi feita ano a ano, com observação quanto ao movimento regulatório estatal e a resposta autorregulatória da plataforma digital. Para fazer esta comparação a plataforma de busca do Google foi utilizada, com o emprego da ferramenta de delimitação de intervalo temporal para a pesquisa, desta forma, foi possível saber, em normas de autorregulação do Twitter que não dispunham de data, qual havia sido a primeira vez que a norma havia sido publicada. A aproximação temporal da publicação dos documentos na plataforma com os projetos de Lei confirma a tese sobre a influência da discussão legislativa, com a elaboração das normas autorregulatórias.

Quando a primeira Política de Privacidade do Twitter (PP) foi publicada, em 2007, o que ela previa estava diretamente relacionado a quatro projetos propostos nas casas legislativas estadunidenses e duas Leis que foram aprovadas e entraram em vigor no ano seguinte. A Internet Freedom Preservation Act (S. 215) propunha a exigência de segurança de rede aos usuários das plataformas digitais e liberdade de

acesso a qualquer tipo de conteúdo, seja pelo formato ou pelas informações contidas. Já o Counter Spy Act (S. 1625) previa criminalizar a instalação de softwares espiões em equipamento alheio, por fim, o Responsible and Effective Solutions for Children Using and Entering Online Services Act (H.R.3850) trazia a necessidade de que as plataformas denunciassem exploradores sexuais, que usassem seus ambientes digitais para aliciar menores.

Ainda em 2007, foi proposta a Broadband Data Improvement Act, convertida na Law Nº 110-385, em 2008. A Lei aprovada anexou no período de discussão o projeto Protecting Children in the 21st Century Act (S. 1965), que previa a criminalização das plataformas digitais que não coibissem a propagação de pornografia infantil. Também discutida em 2007 e aprovada no ano seguinte, a Providing Resources, Officers, and Technology To Eradicate Cyber Threats to Our Children Act - PROTECT Our Children Act - Public Law No: 110-401, abarcou cinco projetos de Lei, que previam, em suma, a proteção de crianças, menores de 12 anos, contra a exposição a crimes sexuais na internet.

A primeira PP do Twitter, resumida no Quadro 7, da página 128, deixou claro a seus usuários que a plataforma digital: 1) faria o monitoramento de atividade ilegal, antiética ou insegura; 2) faria uso de criptografia para que os dados dos usuários fossem mantidos em segurança; 3) poderia compartilhar informações com o governo em investigações policiais sobre atividade ilegal na plataforma; e, 4) trouxe a previsão de que apenas maiores de 13 anos, ou seja, adolescentes, estariam aptos a utilizar os serviços. A idade mínima para utilização da plataforma excluía as crianças, que foram protegidas pelas Leis citadas. Em 2008, nenhum novo instrumento autorregulatório foi publicado pelo Twitter, permanecendo a primeira PP, como documento válido.

Apenas um projeto de Lei estadunidense foi localizado no ano de 2008, dentro do espectro observado por esta tese que engloba liberdade de expressão, privacidade e segurança do usuário, o E-fencing Enforcement Act (H. R. 6713). Este projeto previa a responsabilização das plataformas digitais, caso fossem coniventes com usuários vendedores de produtos roubados. O projeto foi novamente apresentado em 2009, juntamente com o Online Age Verification and Child Safety Act (H.R.4059), que exigia das plataformas digitais meios de fazer a verificação etária dos usuários, com vistas a evitar que menores abaixo de 13 anos tivessem acesso a conteúdo impróprio para a

idade. No mesmo ano, o Twitter publicou a segunda versão da PP e o primeiro Termo de Serviços, que foi atualizado duas vezes em 2009.

As normas autorregulatórias foram atualizadas e a plataforma admitiu que faria não só o monitoramento de atividades, mas também o bloqueio de conteúdo ilegal, ameaçador, difamatório, calunioso, obsceno ou que ofendesse direitos autorais. O Twitter reafirmou novamente a possibilidade de compartilhamento dos dados dos usuários com os governos, em qualquer tipo de investigação. Desde o primeiro TS foi proibida qualquer condução de negócio ilícito, atividade hacker e criação de perfil falso na rede. Ficou previsto o bloqueio ou interrupção de acesso para usuários sob suspeita de atividade ilegal ou imoral na rede. O TS1 reafirmou a obrigatoriedade de no mínimo 13 anos para aderir à plataforma. Na PP2 o Twitter forneceu um endereço de e-mail (privacy@Twitter.com) caso pais ou responsáveis tivessem notícia que seu filho, abaixo da idade permitida, mantivesse uma conta na plataforma. Com a informação, a empresa se comprometia a deletar dados e o perfil do menor.

O ano de 2010 marca a entrada de Brasil e União Europeia na discussão regulatória, que influencia a criação das normas autorregulatórias do Twitter, no período analisado nesta tese, dentro dos temas delimitados. No Brasil foi proposto o PL 7131, que tratava da responsabilização de autores de blogs pelo conteúdo publicado. O Twitter já previa, desde a primeira norma autorregulatória, que o usuário da plataforma era o responsável pelo conteúdo publicado, com base no que os EUA entendiam a partir da Seção 230. Na UE era publicada a Diretiva 2010/13 que tratava da liberdade de expressão e informação para as transmissões de conteúdo audiovisual, inclusive nas plataformas digitais. O Twitter havia publicado, em 2009, o TS1 que classificava o conteúdo postado como informação em qualquer formato (texto, áudio ou vídeo), novamente, o entendimento vinha do regramento estadunidense que classifica o direito à liberdade de expressão do cidadão como fundamental, garantido pela constituição.

Naquele mesmo ano, nos EUA, foi proposto o projeto de Lei Combating Online Infringement and Counterfeits Act (S.3804), que propunha a possibilidade de bloqueio de atividade ilegal nas plataformas digitais. O assunto já havia sido discutido anteriormente, portanto, já figurava no TS1, a proibição de negócios ilícitos no ambiente do Twitter. Em 2011, o número de projetos de Lei apresentados nos EUA somou cinco propostas. Os projetos Do-Not-Track Online Act (S.913) e Do-Not-Track Kids Act (H.R.1895) tratavam da coleta de dados. O primeiro estabelecia regras para

o público em geral e o segundo com relação a adolescentes de 13 a 17 anos. Percebe-se que o resultado da discussão de tais projetos aparece na evolução das normas autorregulatórias de 2012. Nesse ano, a plataforma anunciou a ferramenta Do-Not-Track, na PP6. O instrumento funcionava como uma extensão dos navegadores usada para impedir o envio de *cookies* aos usuários, como forma de monitoramento de atividade online. A plataforma, porém, manteve um aviso de que alguns serviços poderiam apresentar mau funcionamento devido à ativação de tal mecanismo. Nota-se que a ferramenta de retirada de autorização de envio de *cookies* levou o nome dos projetos de Lei propostos.

Ainda em 2011, nos EUA foram propostos Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act - PROTECT IP Act (S.968), o Stop Online Piracy Act (H.R.3261) e o Online Protection and Enforcement of Digital Trade Act – OPEN Act (S. 2029), basicamente as propostas combatiam a pirataria e atividade ilegal em ambiente digital nos EUA. Devido a projetos anteriores, as normas autorregulatórias do Twitter já haviam proibido a utilização da plataforma para postagem de conteúdo ilegal, prevendo, inclusive, bloqueio e exclusão de contas que estivessem usando o ambiente para transações ilegais. Mesmo já tendo tocado nos temas, no TS6 o Twitter reforçou que removeria contas de perfis que criassem riscos legais aos demais usuários.

Naquele ano, entrava em vigor na UE a Diretiva 2011/92/UE que tratava da prevenção à exploração sexual infantil na rede, com obrigações para as plataformas no sentido de evitar que menores fossem expostos a conteúdo impróprio ou que pudessem ser vítimas de aliciamento por abusadores. O que a plataforma implementou, em resposta à diretiva, foi um mecanismo de denúncia de assédio e perseguição de usuário por meio de formulários na seção de Ajuda da plataforma, em 5 de novembro de 2011. No ano de 2013, publica pela primeira vez a norma sobre Como Denunciar Comportamento Abusivo (Twitter, 2022j) que vem sendo atualizada com frequência.

No Brasil, em 2011, discutiu-se o PL 1468, que tratava da necessidade de avisar os usuários que fossem aderir às plataformas digitais, de que conteúdo discriminatório era crime. Desde o TS2, o Twitter reforçou que não endossava opinião de usuários, a plataforma rejeitou a possibilidade de campanhas discriminatórias. Ainda por aqui, entrou em vigor, em 2012, a Lei Carolina Dieckmann (Lei 12.737/2012). A Lei impactou o direito penal brasileiro porque criminalizou a invasão

de dispositivos eletrônicos e a utilização indevida de conteúdo alheio, divulgando material sem consentimento do titular. Quando observamos as normas autorregulatórias publicadas pelo Twitter, percebemos a influência da Lei brasileira na admissão pela primeira vez de a plataforma pagar até US$ 100 pelo uso indevido de conteúdo no TS6, ou remoção de material inapropriado, sem detalhamento da informação, porém, no mesmo documento, a plataforma se eximiu de responsabilidade pelo dano a equipamentos de usuários por acesso a conteúdo danoso, com vírus, por exemplo.

Um outro tema chama a atenção nas normas autorregulatórias do Twitter em 2012, o estabelecimento da corte de São Francisco para resolução de questões judiciais. A sede do Twitter fica em São Francisco, na Califórnia. Neste ano, o PL 4565/2012 propunha que na contratação de provedores de aplicação de internet, ou seja, plataformas digitais, que as demandas judiciais fossem solucionadas no Brasil. A proposta brasileira visava a proteção do consumidor nacional, porém, a proposta não chegou a passar nas discussões legislativas. Enquanto isso, o Twitter indicou aos usuários, em seu TS6, que o foro de discussão de demandas judiciais referentes à empresa seria o de sua sede nos EUA, contradizendo a demanda brasileira, que sem aprovação não teve validade jurídica.

Ainda em 2012, dentro da mesma temática de monitoramento, o projeto de Lei Mobile Device Privacy Act (H.R. 6377) tratou da necessidade de informar usuários sobre a instalação de mecanismos de escaneamento da atividade na rede. A partir desta proposta, percebe-se que houve um detalhamento nas normas do Twitter a respeito de como era feito o monitoramento do usuário via *smartphones*. A PP6 informou que o usuário recebia conteúdo e sugestão de perfis a seguir devido ao seu perfilamento algorítmico, foi ainda pormenorizada a forma de coleta de dados dos usuários de *smartphone*, via *Log Data*, e, por fim, foram apresentados esclarecimentos sobre prestação de informações aos governos por meio administrativo e não apenas judicial. Vale observar que o Twitter anunciou a adesão ao Safe Harbor da UE, na PP6. O Safe Harbor foi acordado entre EUA e UE em 2000, e tratava de padrões de segurança para a integridade e compartilhamento de informações. Com o anúncio, a plataforma atestou que tinha um parâmetro legal para fazer o tratamento de dados de seus usuários.

O ano de 2013 foi marcado pela atualização, nos EUA, da Children 's Online Privacy Protection, a COPPA. A norma exigiu o consentimento parental, para

utilização de serviços digitais, por menores de 13 anos. Como já mencionado, desde a primeira PP, o Twitter havia imposto a idade mínima de 13 anos para utilização da plataforma, assim como o respeito às normas impostas pelo Safe Harbor, que era o acordo entre EUA e UE referente ao tratamento de dados. Na PP7 o Twitter publicou mais um documento avulso sobre como faria o monitoramento de idade. Publicado pela primeira vez em 14 de novembro de 2013, o documento About Age Screening and How it Works (Twitter, 2022 a2) indicava como era a política de rastreio de idade para marcas, para evitar que menores de 13 anos tivessem acesso comercial aos produtos. Além disso, a ferramenta evitava que os menores fossem selecionados para direcionamento de anúncios, ou ainda, tivessem imagens utilizadas para propaganda, o que era proibido pela COPPA (2013) e era tema do projeto de Lei Forbidding Advertisement Through Child Exploitation – FACE Act (H.R.2645, 2013).

Enquanto isso, nas casas legislativas estadunidenses, os parlamentares discutiam dois projetos referentes à proibição de divulgação de dados de geolocalização de usuários. O Online Communications and Geolocation Protection Act (H. R. 983) e o Geolocational Privacy and Surveillance Act – GPS Act (H. R. 1312 / S. 639) se referiam à proibição de divulgação de informações de geolocalização tanto para governos como para plataformas. Desde a primeira PP o Twitter previa que a informação de localização do usuário era utilizada para melhorar a experiência do usuário. A partir da PP6, em 2012, previu o compartilhamento de dados de navegação com as companhias telefônicas, pelo acesso à plataforma via *smartphones*. Neste caso, infere-se que os parlamentares reagiram a um comportamento de monitoramento compartilhado entre operadoras de celular e plataformas digitais. Na PP6, o Twitter adiciona a indicação de que seria possível ao usuário controlar, em suas configurações, o compartilhamento ou não de dados de georreferenciamento.

A legislação brasileira impactou as normas autorregulatórias do Twitter a partir de 2014, com a entrada em vigor do Marco Civil da Internet (Lei nº 12.965, 2014), que ficou em discussão por sete anos nas casas do legislativo brasileiro. O MCI (Lei nº 12.965, 2014) tratou principalmente da privacidade do usuário e um reflexo sentido foi a mudança da política do Twitter com relação ao compartilhamento de dados de seus assinantes com terceiros. O TS8 chegou a apresentar um documento à parte que tratou da temática, pormenorizando como as informações seriam disponibilizadas. O documento à parte foi intitulado de sobre Aplicativos de Terceiros e Sessões de

Acesso (Twitter, 2014). Este instrumento informou aos usuários que era possível personalizar a experiência, autorizando ou não a partilha de dados com terceiros.

Outro instrumento, publicado pela plataforma no ano seguinte à entrada em vigor do MCI (Lei nº 12.965, 2014), foi o Como Controlar a sua Experiência no Twitter (Twitter, 2022u), publicado pela primeira vez em 2015, logo após a Lei brasileira. Basicamente, o Twitter criou uma série de ferramentas de customização de experiência do usuário na plataforma. Estes mecanismos permitiriam ao usuário restringir notificações, silenciar contas que não quisesse visualizar, bloquear perfis para que não pudessem ter acesso ao seu conteúdo, e, ainda, denunciar contas por abuso, assédio, divulgação imprópria. O documento apresentou ainda a possibilidade de impedir marcações, compartilhamento de mídia e localização.

O MCI (Lei nº 12.965, 2014) indicou que a plataforma digital só seria responsabilizada por conteúdo danoso, caso se recusasse a retirar do ar material indicado pela justiça. O TS8 apontou que conteúdo compartilhado seria de responsabilidade do usuário, inclusive quando o material causasse danos a terceiros. Enquanto o MCI (Lei nº 12.965, 2014) entrava em vigor no Brasil, o senado estadunidense discutia a proposta Law Enforcement Access to Data Stored Abroad Act (S.2871) que tratava de requisitos a serem atendidos por agências de investigação que pedissem informações às plataformas digitais. Uma das exigências seria a apresentação de um mandado judicial. Em 2015, o Twitter colocou no TS9 a disposição de que a administração da plataforma poderia acessar informações, ler e até compartilhar dados para cumprimento de ordem judicial.

Ainda em 2014 discutiu-se nas casas legislativas estadunidenses o projeto de Lei Commercial Privacy Bill of Rights Act (H.R.4711 / S.2378), direcionado, principalmente, à comercialização de produtos e serviços com marketing agressivo de recomendação e uso de *spam* e *bots*. A PP9, naquele ano, trouxe um detalhamento minucioso de como era feita a guarda das informações referentes às transações financeiras intermediadas via plataforma. Os usuários comerciais foram citados na norma autorregulatória, porém, sem detalhamento. Um documento adicional chamado de Developer Policy (Twitter, 2014c) foi publicado no fim daquele ano, dando as orientações aos usuários comerciais indicando que encaminhamento de promoções precisavam de consentimento explícito, que em caso de *opt-out* do usuário isso teria de ser imediatamente atendido, era proibido seguimento em massa e uso de *bots*.

Enquanto as casas legislativas brasileiras discutiam o projeto de Lei da LGPD (Lei Nº 13.7096, 2018)e a UE formulava o RGPD, o Twitter começou a preparar terreno em suas normas autorregulatórias. A PP10 tratou conteúdo como divulgação, admitindo que o usuário poderia apenas compartilhar uma informação que não fosse produzida por ele mesmo. Ao mesmo tempo, no TS9, regulou a forma de denunciar usuários por utilização indevida de conteúdo com proteção de direitos autorais. O documento previu ainda a separação dos usuários europeus dos demais, estabelecendo a filial Irlanda, como detentora da responsabilidade de tratamento dos dados dos cidadãos do bloco e destinatária das demandas jurídicas do território, que seriam solucionadas na corte do país europeu.

A plataforma admitiu ainda a possibilidade de uso de pseudônimos nas contas. O Twitter instituiu também a possibilidade de acessar, ler e compartilhar os dados do usuário, de forma discricionária, para cumprir decisão judicial ou governamental. Mas mesmo tendo feito várias mudanças em suas normas autorregulatórias, em 2016 o Twitter precisou fazer mais adaptações a partir da aprovação do Regulamento Geral sobre Proteção de Dados, o RGPD europeu. A norma da UE trouxe muitas mudanças na forma como os dados dos cidadãos do bloco deveriam ser tratados pelas plataformas digitais. O RGPD fez com que o Twitter mudasse em um mesmo ano duas vezes suas Políticas de Privacidade e outras duas vezes seus Termos de Serviços.

Entre o ano anterior e a aprovação do RGPD o Twitter fez 27 mudanças dentro de suas Políticas de Privacidade e Termos de Serviço, referentes aos temas investigados nesta tese. Como o RGPD previu que empresas estrangeiras precisavam manter filial na UE para tratamento de dados de cidadãos do bloco, o Twitter já havia se antecipado, transferindo o controle de dados dos usuários europeus para a filial na Irlanda. Na PP11, o Twitter retirou o Safe Harbor Principles of Privacy como referência de padrão de tratamento de dados e publicou a adesão ao UE-EUA Privacy Shield, que consiste em um programa com parâmetros de transferência de dados entre o bloco europeu, EUA e Inglaterra. Trouxe ainda a possibilidade de resolução de conflitos via JAM e câmaras de arbitragem.

A PP11 e a PP12 trouxeram ao usuário maior responsabilização na postagem de conteúdo, com verificação sobre legalidade do material e oferta de risco a demais assinantes para acesso a links externos. O Twitter trouxe para a PP12 ainda a explicitação de compartilhamento de dados dos usuários com empresas de tendência de mercados, estabeleceu que contas governamentais ou corporativas deveriam

apresentar uma autorização específica de administração. No TS11 impôs regras e responsabilidades para fornecedores de serviços comerciais. Isso porque o RGPD previu que todo o tratamento de dados deveria estar especificado em contrato, sob pena de sanção para uso indevido de informações de usuários, que não estivesse informado.

Além disso, o RGPD previu que o Comitê Europeu para a Proteção de Dados trataria sobre o perfilamento de usuário com base em dados sensíveis como raça, credo, orientação política, entre outros dados que pudessem configurar segregação em caso de utilização para direcionamento de conteúdo. E, neste sentido, o Twitter em sua PP12 restringiu a segmentação de conteúdo por raça, religião, política, vida sexual e saúde e ainda publicou, em dezembro de 2017, a norma complementar Política de Mídia Sensível (Twitter, 2022o). No documento, o Twitter informa que estaria proibida qualquer busca de audiência menor de 13 anos, deixa claras as restrições de conteúdo adulto para menores e proíbe material de violência explícita ou propagação de ódio contra minorias étnicas, sexuais ou religiosas.

Como o RGPD só entrou em vigor em 2018, as mudanças nas normas do Twitter seguiram sendo feitas até a data limite, congregando ainda, modificações a partir da discussão de mais projetos de Leis que estavam sendo discutidos nas casas legislativas de Brasil e EUA. No Brasil, dois projetos de Lei trataram da saúde mental dos usuários das plataformas digitais, apontando para a necessidade de que as redes sociais tirassem do ar conteúdo que promovesse automutilação ou incentivasse o suicídio (PL 7460/2017, PL 7917/2017).

A resposta do Twitter veio com a publicação da Política de Automutilação e Suicídio (Twitter, 2022m), também em dezembro de 2017. Logo no início do documento, a plataforma informa que seria proibido qualquer incentivo à prática da automutilação ou suicídio. A norma trouxe parâmetros do que seriam as publicações que poderiam ativar gatilhos de pessoas suscetíveis a estas práticas. De acordo com o Twitter, a confecção da norma autorregulatória contou com a participação de especialistas da psicologia. Foram considerados gatilhos as publicações de auto inflexão de ferimentos físicos ou comportamentos alimentares tais como bulimia e anorexia.

No sentido de tentar identificar linguagem que incentivasse a prática de automutilação e suicídio o Twitter sinalizou as frases: “’o mais eficiente’, ‘o mais fácil’, ‘o melhor’, ‘o mais bem-sucedido’, ‘você deve’, ‘por que você não faz tal coisa’”, que

foram compreendidas como sinais de alerta. Publicações neste sentido poderiam ser denunciadas e contas que violassem a política encerradas. Debates, conteúdo educativo e mecanismos de prevenção foram excluídos da norma. Uma campanha utilizando as hashtags #DiaMundialDaPrevençãoDoSuicídio, #PrevençãoDoSuicídio, #SetembroAmarelo #WorldSuicidePreventionDay, #WSPD, #WSPD2020, #SuicidePrevention, em 23 idiomas, foi lançada em 2018 e anualmente estaria sendo feita pela plataforma.

Ainda em 2017, nos EUA, figurava em discussão o Online Privacy Act (H.R.3175, 2017; H.R.4978, 2019; H.R.6027, 2021), que impulsionado pelo RGPD discutia a possibilidade de que os EUA implantassem uma Agência de Privacidade de Dados. A resposta na autorregulação do Twitter, ainda impactada pelo RGPD e pela discussão da LGPD (Lei Nº 13.7096, 2018)brasileira, que avançava, trouxe a possibilidade de os usuários fazerem sua personalização de exposição a anúncios, na PP13, assim como foi retirado do documento o monitoramento da plataforma pelo acesso aos ícones de aplicativos no *smartphones*, os chamados *widgets*. O Twitter publicou na PP13 a adesão à Digital Advertising Alliance (DAA), que reúne membros do setor em busca de soluções regulatórias para os problemas relacionados à publicidade online.

Ainda em 2017, entrou em vigor no Brasil a Lei 13.488/2017, que alterou a Lei 9.504/1997 e ficou conhecida como Minirreforma da Lei Eleitoral. A norma tratou dos ambientes online em que os candidatos poderiam fazer campanha, como as redes sociais, caso do Twitter. Compreendeu ainda de que forma poderia ser feita a publicidade digital dos candidatos. A Lei inicialmente fez o Twitter criar um rótulo para os candidatos a presidente, governador e senador, no Brasil[49]. Na leva de normas criadas em dezembro de 2017, o Twitter implementou a Política de Integridade Cívica (Twitter, 2021c). Logo no início do texto, a norma autorregulatória já trazia o alerta de que os perfis não poderiam ser utilizados para manipulação eleitoral ou atos cívicos, independentemente de o usuário ser político ou cidadão comum. O Twitter entendeu como atos cívicos as eleições, censo ou votações como plebiscitos. Comportamento e conteúdo enganoso violariam esta política, incluindo a intimidação de eleitores e a

[49] Sobre os rótulos de eleições no Twitter. 22/06/2018. https://help.Twitter.com/pt/using-x/election-labels Acessado em 21/10/2023.

personificação de candidatos em contas falsas. A norma autorregulatória instituiu canais de denúncia, sobre comportamento infrator.

Preparando-se para entrada em vigor do RGPD, o TS12 do Twitter informou que o conteúdo poderia ser removido não só por infração a direitos autorais, mas também, por *posts* feitos por contas falsas, por conter ilicitude ou se configurar como assédio. Ao mesmo tempo, o documento ofereceu um endereço eletrônico para reclamação sobre remoção de conteúdo. Citou ainda que Leis locais seriam as balizas para que funcionários da plataforma tratassem das reclamações. Além de afirmar, que mudanças nas normas autorregulatórias seriam informadas aos usuários com 30 dias de antecedência. Todas estas diretrizes estavam previstas no RGPD, que entrou efetivamente em vigor em 2018.

Enquanto isso, no Brasil era aprovada a Lei Geral de Proteção de Dados, a LGPD (Lei nº 13.709/2018), que trazia muitos dispositivos consonantes ao RGPD. Além disso, nas casas legislativas brasileiras o PL 10919/2018 discutia a obrigação da identificação dos anúncios publicitários nas plataformas digitais e nos EUA seis propostas legislativas tratavam de assuntos diversos como: consentimento para uso de dados e parâmetros de segurança de tratamento das informações (Consent Act S.2639/H.R.5815, 2018; e Social Media Privacy Protection and Consumer Rights S.2728, 2018; S.189, 2019; S.1667, 2021), obrigação de identificação de *bots* (Bot Disclousure and Accountability Act S.3127, 2018; S.2125/H.R.4536, 2019), criação de site pela FTC para verificação de postagem indevida de conteúdo sexual (Remove Act H.R.6917, 2018, H.R.8013, 2022), desenvolvimento de parâmetros de responsabilidade às plataformas que cuidam de dados (Care Act S.3744,2018; S.2961, 2019; S.919, 2021), e, mudança no entendimento de responsabilização por conteúdo de terceiros de plataformas digitais que faziam direcionamento algorítmico de material (Biased Algorithm Deterrence Act H.R.7363, 2018; H.R.492, 2019).

Diante de tantas demandas, na PP14, em 2018, o Twitter admitiu a venda de dados e monitoramento das atividades até mesmo dos anunciantes. Admitiu algo que todos sabiam que ela fazia. Na tentativa de reduzir o dano, possibilitou o bloqueio de direcionamento por perfilamento algorítmico. A PP14 informou ainda sobre a criação do Data Protection Office, para os usuários da UE. Foi a primeira vez que o Twitter pediu a opinião dos usuários sobre a Política de Privacidade que vinha sendo aplicada na plataforma. Trouxe a opção de os usuários fazerem sua própria configuração de segurança. A portabilidade dos dados, regra presente no RGPD e na LGPD (Lei nº

13.709/2018), entrou na norma autorregulatória, com a indicação de um link para checar qual era a legislação vigente para tratamento de suas informações, segundo sua localização.

Ao final de 2018, entrou em vigor nos EUA a Allow States and Victims to Fight Online Sex Trafficking Act - Public Law No. 115-164 (04/11/2018), que tratou do combate ao tráfico sexual de pessoas e vítimas de exploração sexual. No ano seguinte, as casas legislativas discutiram pela primeira vez o projeto de Lei END Child Exploitation Act (H.R.5376 / S.3007, 2019; H.R.3538 / S.365, 2021) propondo que as plataformas digitais conservassem, por 90 a 180 dias, conteúdo denunciado por exploração sexual infantil. A conservação do material era indicada como fundamental para investigação da conduta ilegal. O Twitter explicou na PP14, que os dados dos usuários seriam mantidos por 18 meses, até mesmo quando a conta fosse excluída.

Ao final de 2017, quando a Lei ainda estava sendo discutida, a plataforma publicou a Política Relacionada à Nudez Não Consensual (Twitter, 2019d), que trouxe parâmetros sobre publicação de fotos ou vídeos com conteúdo sexual explícito ou implícito, sem o consentimento dos retratados no material. Foram classificados neste contexto material capturado com câmera escondida, ou em ambiente íntimo não destinado a divulgação pública, assim como manipulações de imagens, com substituição de rosto. Qualquer conteúdo neste sentido poderia ser denunciado, em canais específicos. Foi excluído da norma material sexual consensualmente produzido para divulgação.

Outra norma autorregulatória que compreendeu as exigências legislativas anteriores foi a política sobre Produtos ou Serviços Ilegais ou Regulamentados (Twitter, 2019d), que incluíam a proibição de veiculação de conteúdo referente a falsificação, produto controlado, tráfico humano, espécies protegidas, serviços sexuais, produtos roubados, armas de fogo e munição. A norma autorregulatória englobou, inclusive, a reivindicação da proposta legislativa estadunidense Combating Online Wildtrafficking Act (H.R.5398, 2019; H.R. 1546, 2021), que tratava da comercialização online de produtos advindos do tráfico de animais. E, ainda, o Regulamento (UE) 2019/1150, que instituiu as bases para o relacionamento entre plataformas e fornecedores de produtos, ou serviços online.

O Regulamento (UE) 2019/1150 entrou em vigor em conjunto com a Diretiva 2019/790. A Diretiva estava voltada às normas sobre os direitos autorais, já o Regulamento estabeleceu a equidade de direitos e deveres de plataformas e usuários

profissionais. Apesar do Twitter já ter adiantado algumas questões referentes a relacionamentos comerciais e direitos de autor na PP14, a plataforma publicou a Política de Marcas Registradas (Twitter, 2019c). Neste documento, detalhou o que entendia por violação de direito autoral e de marcas, criando inclusive a possibilidade de denúncia por uso indevido do bem protegido. A PP15 classificou como apropriação indébita a utilização de material protegido por marca. Complementarmente criou, no mesmo ano publicou a Política de Contas de Paródias, Comentários e Fã-Clubes (Twitter, 2022z), detalhando em quais contextos seria possível utilizar conteúdo protegido, sob a forma de comentário, análise ou esquete.

Ainda em resposta ao Regulamento (UE) 2019/1150, o Twitter estabeleceu, em 2020, por meio da Amplify Publisher FAQs (Twitter, 2022d2), quais seriam os conteúdos passíveis de monetização e como se daria o recebimento de valores. De acordo com a norma, apenas depois dos 18 anos seria possível ter uma conta profissional, verificada e apta a receber monetização. Todo o conteúdo seria revisado e materiais violentos, sexuais ou com temática sensível não seriam passíveis de monetização. Basicamente a norma explicava ao autor como ele seria pago, com que frequência receberia os dividendos pelo conteúdo e como reclamaria em caso de não recebimento dos valores julgados devidos. O usuário profissional poderia impedir a veiculação de propagandas, em seu conteúdo, por tema e marca. O Twitter reservou um endereço de e-mail para contato em caso de problemas com pagamento.

Com relação à venda de produtos, a PP15 previu que os usuários profissionais teriam a obrigação de anuir com o compartilhamento de dados de transações financeiras. Dois anos depois, a PP17, abriu a possibilidade de uso profissional do Twitter, com categorização da atividade, deixando abertos dados como nome, endereço, contato telefônico e de e-mail. Também foi estabelecido que a exclusão de conta profissional a pedido do usuário teria de vir acompanhada de uma comprovação de domínio do perfil.

Percebe-se que em 2019 o Twitter respondeu às mudanças ou discussões legislativas apenas com documentos individualizados sobre as temáticas trazidas nas propostas. Portanto, PPs e TSs, não foram alterados, mesmo com discussões de três projetos de Lei no Brasil e mais 11, pela primeira vez, nas casas legislativas dos EUA. A maior parte das temáticas discutidas nos projetos legislativos do Brasil e EUA já tinham sido tratadas em normas autorregulatórias. Caso da regulação de conteúdo terrorista como proposto pelo PL 2463/2019 que dispunha sobre a limitação de

divulgação de imagens de ataques massivos ou de dois projetos dos EUA que seriam o National Commission on Online Platforms and Homeland Security Act (H.R.4782, 2019) e o Raising the Bar Act (H.R.5209, 2019).

O Twitter, porém, respondeu ao anseio legislativo reforçando seu entendimento sobre conteúdo terrorista a partir da publicação da Política Contra Organizações Violentas (Twitter, 2020g). A norma autorregulatória tratou não só de terrorismo, mas também de outros tipos de organizações violentas que visavam a segregação de povos ou minoras. Os *posts* educativos sobre a temática foram considerados exceção à regra, porém, as demais publicações acabaram figurando para julgamento dos usuários, que poderiam denunciar condutas infringentes, com possibilidade de exclusão das publicações.

A partir de 2020, o Brasil colocou a LGPD (Lei Nº 13.7096, 2018)em vigor. A norma trouxe o regramento de tratamento dos dados dos cidadãos brasileiros, porém, grande parte dos temas discutidos na LGPD (Lei Nº 13.7096, 2018)já haviam sido modificados nas normas do Twitter devido à entrada em vigor do RGPD europeu. Como as normas legislativas brasileira e europeia coadunam em seu teor, não foram notadas mudanças nas PPs e TSs, com relação às temáticas propostas pela LGPD (LEI Nº 13.709/2018). Enquanto a LGPD (Lei Nº 13.7096, 2018)entrava em vigência, outros sete projetos de Lei foram apresentados na Câmara e Senado do Brasil, entre eles o PL 2630/2020, conhecido como PL das Fake News, cuja última versão, agregando 73 projetos de Lei, tratou insistentemente sobre a moderação de conteúdo.

Enquanto isso, nos EUA 25 novos projetos legislativos figuraram pela primeira vez na Câmara dos Representantes e Senado, 13 propostas trataram da remoção ou relativização da imunidade das plataformas digitais, pela moderação de conteúdo. Nota-se que neste período a moderação de conteúdo passou a figurar como tema chave na maior parte dos projetos legislativos, referentes à regulação das plataformas digitais. Como resposta, o Twitter publicou na PP15 um alerta ao usuário sobre sua concordância com o *post* e anuência em aumento da distribuição em caso de compartilhamento de conteúdo, ou seja, a plataforma colocava também sob a responsabilidade dos assinantes a propagação das mensagens mais visualizadas nas *timelines*. O documento informou aos usuários que o Twitter poderia remover *posts* com glorificação de violência.

Para detalhar o tema, o Twitter publicou uma série de documentos avulsos, ainda em 2019, para delimitar o que seria conteúdo indesejado dentro da plataforma.

Nesta linha foram publicados a Política Contra a Glorificação da Violência (Twitter, 2019b) e até mesmo Normas para Monetização de Conteúdo (Twitter, 2022c2). O Twitter detalhou que a ameaça de pessoa ou grupo de pessoas, minorias, seria considerado conteúdo violento e exemplificou: “glorificar, comemorar, elogiar ou tolerar crimes e eventos violentos em que pessoas foram vítimas por pertencerem a um grupo protegido ou os autores de tais atos”. O documento citou ainda que elogio ou comemoração de ato terrorista ou antissemita estariam incluídos como conteúdo vetado por estas políticas. Não estariam incluídos, segundo esta política, *posts* com opiniões sobre guerras entre Estados constituídos.

No TS14, o Twitter admitiu que vinha fazendo a curadoria do conteúdo e ainda deixou claro que a restrição de distribuição ou limitação de visualização de *posts* seria feita de forma discricionária pela plataforma. Outras normas autorregulatórias foram postadas pela empresa para direcionar o caminho que estava seguindo para diferentes tipos de conteúdo, prevendo restrições para material ofensivo. Neste sentido, publicou a norma Sobre Assédio Online (Twitter, 2022i), na qual instruiu os usuários a documentarem comportamento abusivo e intimidatório, para garantir punição aos responsáveis, dando à plataforma a identificação da conta que perpetrou o insulto. E ainda publicou Como ajudar um Usuário de Assédio Online (Twitter, 2022k), no qual instrui outros usuários a denunciar situações de assédio na rede.

Ainda em 2020, dois projetos de Lei estadunidense focaram novamente em *posts* sobre exploração sexual infantil (Eliminating Abusive and Rampant Neglect of Interactive Technologies Act – EARN IT Act - S.3398 / H.R.8454, 2020; Invest in Child Safety Act - S.3629 / H.R.6752, 2020). Em resposta, o Twitter publicou a Política Contra a Exploração de Menores (Twitter, 2020h), declarando tolerância zero a este tipo de conteúdo. Qualquer formato de mídia, com publicações ainda que geradas por computador, como ilustrações, sobre o tema, seria retirado do ar. Vários outros comportamentos pormenorizados foram citados na política como intoleráveis, mediante a norma autorregulatória.

Outras duas propostas legislativas estadunidenses previam criminalização de contas falsas (Social Media Accountability na Account Verification H.R.6587, 2020; H.R. 4564, 2021; Social Media Fraud Mitigation S.3629/H.R., 2020; H.R.807/S.223, 2021) o Twitter reiterou em sua PP15 que os usuários poderiam ter contas diversas para expressar diferentes pontos de vista. Paralelamente um outro documento avulso foi publicado na plataforma sob o título Política de Identidades Enganosas e que

Induzem ao Erro (Twitter, 2022i). Nesta outra norma a plataforma reiterou a intenção de que seu ambiente online fosse de divulgação de ideias, porém, sem ilusão ou personificação falsa de pessoas ou instituições e explicitou “é proibido apropriar-se indevidamente da identidade de outros grupos, pessoas ou empresas ou criar identidade falsa para fins de induzir outros ao erro”. Desta forma, foi proibido identificar o usuário como entidade ou pessoa não associada ao dono da conta.

Em 2021, a UE atualizou a sua norma sobre a moderação do conteúdo terrorista com o Regulamento (UE) 2022/784, complementando a Diretiva 2017/541. Como resposta, o Twitter publicou mais uma norma avulsa a Política para Autores de Ataques Violentos (Twitter, 2022a). O documento exemplifica quais condutas do usuário seriam consideradas inapropriadas, como ataques terroristas, ataques extremistas violentos ou ataques violentos em massa, com postagem de ações. O manifesto foi considerado uma declaração, na qual o indivíduo justificava a violência perpetrada. A medida corretiva proposta era a exclusão da conta para evitar a disseminação do conteúdo.

Enquanto isso, no Brasil, três projetos de Lei trataram da moderação de conteúdo, entre eles, o PL 3700/2021, que propunha a moderação de discurso de ódio. A Política contra a Propagação de Ódio (Twitter, 2022h) foi publicada pormenorizando os comportamentos que seriam indicados como de propagação do ódio. Entre eles, o desejo de morte ou violência gratuita aos usuários. Além da incitação para práticas violentas contra pessoas ou grupos específicos.

Nos EUA as casas legislativas apresentam pela primeira vez 18 propostas de legislação com foco, também em moderação de conteúdo, sendo sete delas voltadas à responsabilização das plataformas que interferissem no ponto de vista do usuário por remoção ou redução de distribuição de conteúdo protegido pela constituição. Observando o movimento polarizado nos projetos legislativos, que hora propunham a retirada de imunidade da plataforma por remoção de conteúdo legal e hora penalizavam as redes pela inércia na moderação, o Twitter propôs em 2021 a criação de comunidades. Nestas comunidades seria possível participar de discussões com pares semelhantes[50].

[50] Comunidades do Twitter. Disponível em: https://help.Twitter.com/pt/using-x/communities Acessado em 28/10/2023.

As discussões sobre moderação de conteúdo estiveram presentes em anos anteriores, portanto, pouco destas discussões legislativas de 2021 se refletiram nas nas PPs e nos TSs do Twitter. Estes documentos foram reservados apenas para normas voltadas a informações básicas, sobre moderação de conteúdo se limitaram a dizer que haveria possibilidade de transcrição de material publicado em áudio, para compartilhamento em forma de texto. Complementarmente o Twitter publicou o documento Sobre Conteúdo Ofensivo (Twitter, 2022l), que foi uma preocupação presente nos projetos de Lei de 2021 tanto no Brasil, quanto nos EUA. A norma autorregulatória explicou o que o Twitter compreendia como conteúdo ofensivo. O primeiro alerta era sobre a responsabilidade de quem fizesse o tweet, observando sentido ofensivo ou prejudicial da linguagem. O segundo alerta era voltado ao Leitor, que compreendesse o contexto antes de fazer qualquer denúncia. Para interações negativas, a plataforma abriu a possibilidade de bloqueio de contas ofensivas, além da denúncia por conteúdo impróprio.

Quando observadas as temáticas dos projetos legislativos sobre moderação de conteúdo, nota-se que três propostas estadunidenses trataram de moderação de conteúdo para salvaguardar menores ou indivíduos com condições especiais, que pudessem ser mais impactos por conteúdo violento ou impróprio (Promoting Rights and Online Speech Protections to Ensure Consume ris Heard Act – Pro-Speech Act S.2031; Federal Big Tech Tort Act H.R.5449 / S.2917; Justice Against Malicious Algorithms Act H.R.5596; Nudging Users to Drive Good Experiences on Social Media – Nudge Act S.3608).

Da mesma forma, no Brasil, o projeto 3700/2021 propunha obrigações e moderação de discurso de ódio. Em resposta, o Twitter publicou o documento Política sobre Mídia Sensível (Twitter, 2022o). O documento especificou que era proibida a publicação de conteúdo sangrento, violento, adulto ou de ódio em vídeos ao vivo. Vários tipos de postagens foram determinados como proibidos ou impróprios para menores. Neste sentido, a plataforma deixou claro que não seria distribuído para usuários menores e nem para aqueles que não informaram a idade de qualquer material desta natureza.

Outro documento que contemplava a demanda dos legisladores era a Política de Mídia Sintética e Manipulada (2021), na qual ressaltou que mídias manipuladas poderiam dar ideias enganosas aos usuários. A plataforma ponderou, porém, que correções de cores e utilização de filtros não indicariam qualquer malefício. Estariam,

neste quesito, passíveis de moderação, com remoção de conteúdo ou redução de distribuição das mídias sabidamente manipuladas para enganar os usuários, propagando inverdades ou expondo indivíduos a risco de violência. Estariam fora do escopo da norma, mídias de sátiras, contradiscursos, comentários, animações.

O ano de 2022 foi marcado pela entrada em vigor, na UE, do Regulamento (UE) 2022/991, que trouxe as diretrizes para o tratamento de dados em casos de investigações da Europol, com cooperação das plataformas digitais. O Twitter publicou em seu TS17 algumas questões que estavam ligadas à segurança, como a proibição de personificação de outras pessoas na plataforma. E, ainda, classificou como falsidade ideológica a montagem de perfis *fakes*. Além disso, proibiu o usuário de fazer alterações técnicas na API da plataforma, em busca de criar limitações técnicas.

Também passou a valer o Regulamento (UE) 2022/1925 que tratou das regras de equidade do mercado digital e o Regulamento (UE) 2022/2065 que estabeleceu as normativas para a oferta dos serviços digitais. Algumas normas do Twitter já tinham regras previstas nestas legislações, caso da norma que tratou sobre Produtos ou Serviços Ilegais ou Regulamentados (Twitter, 2019d). Com referência aos produtores de conteúdo digital, o Twitter publicou o documento Normas para Monetização de Conteúdo (Twitter, 2022c2), reconhecendo a possibilidade de monetização de conteúdo apenas de usuário maior de 18 anos, em área possível de recebimento de valores, com contas verificadas, assinantes há pelo menos três meses.

Foi estabelecido que o Super Follows (Twitter, 2022e2) e Política de Espaços com Ingressos (Twitter, 2022g2) seriam os serviços destinados à monetização de conteúdo. Na mesma linha, voltado aos criadores de conteúdo, o Amplify pre-roll Publisher Program FAQs (Twitter, 2022d2) estabeleceu regras de pagamento para usuários profissionais por produtos ou serviços oferecidos via plataforma. O documento detalha periodicidade de envio de valores, a quem e como reclamar em caso de atraso ou não envio dos valores.

De acordo com os documentos de venda de produtos e serviços no Twitter, a plataforma elencou várias classes de produtos que seriam proibidas de anúncio de comercialização via plataforma do Twitter como conteúdo adulto, bebida alcóolica, animais vivos ou em extinção, apostas, imóveis entre outros. Além das normas autorregulatórias atender à demanda dos Regulamentos 2022/1925 e 2022/2065 da UE, englobou ainda projetos de Lei em discussão nos EUA que propuseram

legislações como a Accountability for Online Firearms Marketplaces Act (S.2725 / H.R.7819, 2022), que previa a retirada de imunidade de plataformas que intermediassem comercialização de armas.

Outra discussão muito presente em 2022, nos EUA foi a privacidade do usuário estadunidense, a temática apareceu em três propostas: Digital Platform Commission Act -S.4201 / H.R.7858; Public Servant Protection Act - S.4965; American Data Privacy and Protection Act - H.R.8152, 2022. A última proposta legislativa era muito semelhante ao RGPD europeu e à LGPD (Lei Nº 13.7096, 2018)brasileira. Com relação à privacidade, o Twitter abriu aos usuários a possibilidade de fazerem questionamentos sobre a política implementada pela empresa na PP18.

Dentro das especificações do documento Como Proteger e Desproteger seus Tweets (Twitter, 2022x) foi detalhado que estaria proibida a divulgação de dados dos usuários e a ameaça de fazê-lo. Além disso, dentro do critério privacidade foi estabelecido que o compartilhamento de mídia privada, sem consentimento, também não seria permitido. O usuário recebeu a possibilidade de bloquear marcações, ficar invisível para quem não fosse seguidor e ainda evitar que seus tweets pudessem identificar sua localização de postagem, preservando seu georreferenciamento.

Atendendo às demandas de privacidade o Twitter publicou Como Controlar sua Experiência no Twitter (Twitter, 2022u), no qual trouxe dicas aos usuários de como preservar dados, filtrar notificações, silenciar contas, controlar conteúdo de visualização em sua *timeline*. Deixou claro como os dados são utilizados para recomendação de conteúdo no documento Política contra Spam e Manipulação da Plataforma (Twitter, 2022c), que também detalhou a proibição sobre campanhas publicitárias com envio de mensagens em massa de propaganda, ou menção de pessoas aleatórias e ainda engajamento não autêntico com uso de *bots*. O Twitter pormenorizou uma prática conhecida que seriam perfis sobrepostos, que interagem mutuamente, com conteúdo idêntico para inflar métricas e isso foi demarcado como conduta proibida.

Já com relação à segurança do usuário entrou em vigor a Diretiva (UE) 2022/2555, que foi uma atualização de padrões para a normatização de legislações sobre cibersegurança nos países do bloco europeu, ressaltando os riscos de ataques como *ransonware*. Com relação à segurança dos dados, o documento Sobre Segurança da Conta (Twitter, 2022r), que havia sido publicado em 2021 pela primeira vez, trouxe ao usuário dicas de como fazer uma senha forte, com 10 caracteres,

misturando letras e números, para evitar invasão. Outra medida instituída pela plataforma para evitar invasão de contas e roubo de dados foi a verificação em duas etapas, com senha e envio de chaves de segurança via celular.

As publicações de normas extra PP e TS atenderam também demandas legislativas como os projetos American Data Privacy na Protection Act (H.R.8152) e o Countering Foreign Malign Influence (H.R.8409). O primeiro focado na proteção dos dados dos cidadãos americanos e o segundo na prevenção à influência manipuladora via plataforma digital por nações estrangeiras. No Brasil, as normas atenderam ao projeto 188/2022, que propunha o combate às informações falsas na rede. Quanto aos projetos 397/2022 e o 630/2022, que obrigariam plataformas transnacionais que tivessem escritórios no Brasil, o Twitter dispunha de sede no país, com CNPJ registrado e base de funcionários em território nacional, inclusive, desde 2012.

CONCLUSÃO

Num mundo cada vez mais dependente da comunicação mediada por aparatos tecnológicos fica difícil imaginar como seriam as interações humanas sem as plataformas de mídias sociais. Nesta realidade informacional ubíqua, a internet é uma ferramenta que perpassa todas as formas de relações humanas da atualidade. Está presente na comunicação em rede, obrigando os cidadãos a se adaptarem às novas formas de convivência digital.

Para que praticamente todas as atividades humanas de interação fossem transportadas para o ciberespaço, a internet evolui em fases, chegando à atual de plataformização das relações pessoais, profissionais e comerciais. Abrindo um leque de possibilidades de influenciar pessoas, numa nova etapa da comunicação de massa, que sai do domínio de monopólios locais de conglomerados de mídia e evolui para os oligopólios transnacionais das plataformas digitais.

Em uma das maiores plataformas de mídias sociais, o Twitter, que mudou de nome para X, em 2023, o texto de apresentação dizia que o ambiente digital era o lugar certo para saber mais sobre o que estava acontecendo e sobre o que as pessoas estavam falando. O Twitter reiterava que liberdade de expressão era um direito humano fundamental. Porém, na plataforma, a liberdade se restringia ao que a política da empresa entendia como conversas saudáveis. Esta norma autorregulatória fazia parte de um aparato de regras que a plataforma desenvolveu em normas autorregulatórias, com estabelecimento de parâmetros a serem seguidos pelos seus usuários.

Esta tese defende a premissa de que a autorregulação das plataformas digitais é impulsionada pelo movimento legislativo de regulação. Neste sentido, o movimento autorregulatório é precedido pela discussão legislativa de determinado tema. Para atestar tal tendência, foram selecionados 78 documentos de autorregulação do Twitter e discussões legislativas, com algumas normas convertidas em Leis que somaram 143 instrumentos legais de Brasil, Estados Unidos e União Europeia. O marco temporal analisado foi de 2006, data da criação do Twitter, a 2022, encerramento da plataforma, antes de sua venda e mudança de nome para X.

Foram tratados nesta tese a elaboração de mecanismos de autorregulação e regulação legislativa para os temas: liberdade de expressão, privacidade e segurança do usuário. Estas temáticas foram selecionadas porque fazem parte da Declaração

Universal dos Direitos Humanos, aprovada em 1948, sob a perspectiva de que não é possível avançar nas sociedades democráticas quando direitos básicos estabelecidos deixam de ser respeitados.

É necessário que o arcabouço legal proteja as nações democráticas, garantindo a livre manifestação do pensamento, com manutenção da responsabilização pela prática de crimes. Mesmo em tempos de redes sociais, em que grande parte da vida é vivida publicamente de forma virtual, a privacidade precisa ser preservada. Por fim, nesta nova forma de viver o cotidiano, a criminalidade mudou de abordagem, com riscos que podem estar do outro lado do mundo e crimes que são perpetrados por um clique, portanto, segurança é um ativo com novos desafios.

Os resultados demonstraram que a discussão legislativa tem funcionado como uma alavanca que impulsiona a plataforma digital a normatizar seu comportamento e ação diante dos usuários. Notou-se que inicialmente as normas autorregulatórias do Twitter eram tratadas em dois documentos: Política de Privacidade e Termos de Serviços. Ambos eram atualizados conforme havia discussões nas casas legislativas, ou Leis eram aprovadas e entravam em vigor, porém, com o passar dos anos e da multiplicação dos projetos legislativos, as normas autorregulatórias foram sendo distribuídas em documentos avulsos na plataforma digital.

Para atestar tal tendência, o cruzamento de propostas legislativas e normas autorregulatórias foi feito ano a ano. E desde o início, as primeiras normas autorregulatórias criadas pelo Twitter já tinham como base as Leis propostas pelos legisladores. A primeira Política de Privacidade, de 2007, trazia regras que faziam referência ao conteúdo de quatro projetos de Leis propostos nas casas legislativas estadunidenses e duas Leis que foram aprovadas, entrando em vigor no ano seguinte. A partir daquele ano, os movimentos legislativos precediam a elaboração das normas autorregulatórias. Como se os instrumentos criados pelas plataformas fossem uma resposta às propostas dos legisladores.

Este movimento foi notado com maior influência das casas legislativas estadunidenses, porém, não somente por lá, mas também quando legisladores de Brasil e União Europeia passaram a discutir de forma mais intensa os temas ligados à regulação das plataformas de mídias sociais. Notou-se, por exemplo, grande influência do Marco Civil da Internet (Lei 12.965, 2014), do RGPD (2016) europeu e da LGPD (Lei Nº 13.709, 2018) brasileira sobre normas autorregulatórias do Twitter, com aumento da preocupação com regras de privacidade e segurança do usuário.

Estas legislações trouxeram parâmetros claros de guarda dos dados pessoais dos usuários das redes, que foram sendo refletidos nas normas autorregulatórias publicadas pelo Twitter a partir da discussão e entrada em vigor das Leis. Apesar de os EUA não ter conseguido aprovar legislação semelhante, os cidadãos estadunidenses foram impactados pelas mudanças feitas pelo Twitter em suas normas autorregulatórias devido ao movimento legislativo de Brasil e UE. Neste sentido, a privacidade do usuário avançou quanto ao tratamento dos dados tanto pelas plataformas quanto por governos.

Na questão da segurança é possível destacar avanços em questões como a proteção de crianças nas redes pelo movimento legislativo estadunidense com a atualização da COPPA (2013), entrada em vigor da Allow States and Victims to Fight Online Sex Trafficking Act (H.R.1865, 2013) e a propositura de projetos de Leis referentes ao tema. O Brasil e a UE foram menos profícuos neste tema, porém, também apresentaram iniciativas como a Directiva 2011/93 na UE e no Brasil o PL 2184, 2019. A autorregulação, devido a propositura de Leis contrárias ao monitoramento dos cidadãos como a Do-Not-Track Act (S.913, 2011; S.418, 2013; S.2404, 2015), fez o Twitter criar mecanismos que impedem a coleta de dados de menores. Além disso, foram instalados filtros que impedem a visualização de mídia sensível, com conteúdo violento ou sexual, sem que o usuário concorde antecipadamente com a exposição ao tema.

A moderação de conteúdo é o tema que mais desafia o movimento regulatório, apesar dos avanços registrados. Conteúdo terrorista foi tema principal de pelo menos três propostas legislativas estadunidenses, entre elas a Protecting Americans from Dangerous Algorithms Act (H.R.8636, 2020; H.R.2154, S.3029, 2021) e ainda de legislações da UE como a Directiva 2017/541 e o Regulamento (UE) 2021/784. Trazendo avanços para a retirada de conteúdo desta natureza num prazo rápido de uma hora para as grandes plataformas e no máximo 12 horas para as menores.

Conteúdo ilegal foi o foco principal de pelo menos cinco propostas estadunidenses como a Cooperation Among Police, Tech, and Users to Resist Exploitation Act - CAPTURE Act (H.R.6755, 2022) que propôs a criação de um mecanismo de cooperação entre plataformas digitais e forças de segurança. Proposta semelhante ao Regulamento (UE) 2022/991 que também cria formas de cooperação entre a Europol e as plataformas com vistas a dirimir crimes praticados online. O

Twitter respondeu positivamente com normas que dificultam a distribuição de conteúdo ilícito.

Como já visto, conteúdo sexual tem regras específicas, com liberação de divulgação apenas de material produzido com esta finalidade, que tenha o consentimento dos participantes. Material de extrema violência e discurso de ódio já tem regramento específico e proibitivo da plataforma. Assim como de material ilegal ou que infringe legislação de direitos autorais. Mesmo com estes avanços, ainda há searas a tratar, principalmente referente à compreensão do que seria a liberdade de expressão online. O ponto de equilíbrio entre liberdade de expressão, com responsabilização dos excessos ainda não foi encontrado, porém, segue-se nesta busca.

Referências

ADORNO, Theodor; HORKHEIMER, Max. A indústria cultural: o iluminismo como mistificação das massas. **Indústria cultural e sociedade.** São Paulo: Paz e Terra, p. 7-74, 2021.

ALMEIDA, Denise; SHMARKO, Konstantin; LOMAS, Elizabeth. *The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks*. **AI and Ethics**, p. 1-11, 2022. Disponível em: https://link.springer.com/article/10.1007/s43681-021-00077-w Acessado em: 26/08/2022.

ALTMAN, Sam. *OpenAI CEO, CTO on risks and how AI will reshape society*. [Entrevista concedida a Rebecca Jarvis]. **ABC News**, 17 mar. de 2023. Disponível em: https://www.youtube.com/watch?v=540vzMlf-54 Acessado em: 26/06/2023.

CAPANEMA, Walter Aranha. A responsabilidade civil na Lei Geral de Proteção de Dados. **Cadernos Jurídicos: Direito Digital e proteção de dados pessoais**, ano, v. 21, p. 163-170, 2020.

ALNAJAFI, Nada. Twitter Terms of Service. Law Insider, 19 fev. 2021. Disponível em: https://www.youtube.com/watch?v=RMlkr2dckSU Acessado em 18/09/2022.

AMATO, Lucas Fucci *et al.* Fake news e eleições: estudo sociojurídico sobre política, comunicação digital e regulação no Brasil. Porto Alegre: Editora Fi. Disponível em: https://www.editorafi.com/203fakenews. Acesso em: 02/10/2022

ANANNY, Mike; CRAWFORD, Kate. *Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability*. **new media & society**, v. 20, n. 3, p. 973-989, 2018.

ASSEMBLY, UN General *et al.* Universal declaration of human rights. **UN General Assembly**, v. 302, n. 2, p. 14-25, 1948.

BALLESTEROS, Patricia Tapia. Estrategia de la UE para una lucha más eficaz contra el abuso sexual de menores. **Revista de Estudios Europeos**, n. Extraordinario monográfico 1, p. 434-451, 2023. Disponível em: https://revistas.uva.es/index.php/ree/article/view/7325/5229 Acessado em 11/11/2023.

BALKIN, Jack M. *Digital speech and democratic culture: A theory of freedom of expression for the information society*. In: **Law and Society Approaches to Cyberspace**. Routledge, 2017. p. 325-382.

BARBOSA, Bia. Regulação da mídia, conversa com Bia Barbosa sobre radiodifusão e internet. [Entrevista concedida a Cláudia Abreu, Hélcio Duarte e Rodrigo Otávio]. **Jornalistas em Luta**, 30 mai. 2022. Disponível em: https://www.youtube.com/watch?v=PWlNetnAuaM Acessado em: 24/08/2022.

BARKLEY, Taylor. *What Should Policymakers Do about Social Media and Minors?* **The Center for Growth and Opportunity**, 2023. Disponível em: https://www.thecgo.org/research/what-should-policymakers-do-about-social-media-and-minors/ Acessado em: 13/06/2023.

BARRETO JUNIOR, Irineu Francisco; SAMPAIO, Vinícius Garcia Ribeiro; GALLINARO, Fábio. Marco Civil da Internet (Lei 12.965, 2014) e o direito à privacidade na sociedade da informação. **Direito, Estado e Sociedade**, v. 52, p. 114-133, 2018.

BELLI, Luca. Como combater o aumento das campanhas de desinformação no mundo. [Entrevista concedida a Mariana Trigo]. Bate Papo FGV, 6 nov. 2019. Disponível em: https://www.youtube.com/watch?v=1fFfR6B60EY Acessado em: 24/08/2022.

BELLI, Luca; FRANCISCO, Pedro Augusto; ZINGALES, Nicolo. 25 *Law of the Land or Law of the Platform? Beware of the Privatisation of Regulation and Police.* INTERNET GOVERNANCE AND REGULATIONS IN LATIN AMERICA, p. 423, 2017.

BENEDEK, Wolfgang; KETTEMANN, Matthias C. ***Freedom of expression and the internet: Updated and revised 2nd edition***. Council of Europe, 2020.

BERNERS-LEE, Tim. *I invented the web. Here are three things we need to change to save it*. **The Guardian**, v. 12, 2017.

BIRNBAUM, Emily. *What Is the SMART Act?* [Entrevista concedida a Jason Howell and Mikah Sargent]. **TWiT Tech Podcast Network**,1 ago., 2019. Disponível em: https://www.youtube.com/watch?v=o001s-n-etE Acessado em: 16/06/2023.

BIZBERGE, Ana; MASTRINI, Guillermo; GÓMEZ, Rodrigo. *Discussing internet platform policy and regulation in Latin America.* **Journal of Digital Media & Policy**, v. 14, n. 2, p. 135-148, 2023.

BLACKBURN, Marsha; BLUMENTHAL, Richard. *EXCLUSIVE: Sens. Blackburn and Blumenthal Join Forbes to Discuss Bill to Keep Kids Safe Online*. [Entrevista concedida a Brittany Lewis]. **Forbes Breaking News**, 16 mar. 2023. Disponível em: https://www.youtube.com/watch?v=y8UsgNcOwho Acessado em: 13/06/2023.

BOLAÑO, César. Economia política da internet, mediação e jornalismo: para a crítica da comunicação e da tecnologia. **Eptic online: revista eletrônica internacional de economia política da informação, da comunicação e da cultura**, v. 20, n. 3, p. 135-155, 2018. Disponível em: https://dialnet.unirioja.es/servlet/articulo?codigo=6858561 Acessado em: 11/08/2021.

BOLAÑO, César Ricardo Siqueira *et al.* Aportes teórico-conceituais de Valério Cruz Brittos à Economia Política da Comunicação. **Liinc em Revista**, v. 16, n. 1, p. e5120-e5120, 2020. Disponível em: http://revista.ibict.br/liinc/article/view/5120 Acessado 15/08/2021.

BOSSIO, Diana. ***Journalism and social media: Practitioners, organisations, and institutions.*** Springer, 2017.

BOSTOEN, Friso. *Neutrality, fairness, or freedom? Principles for platform regulation.* **Principles for Platform Regulation (March 31, 2018). Internet Policy Review,** v. 7, n. 1, p. 1-19, 2018. Disponível em: Acessado em: 02/06/21.

BOURREAU, Marc; DE STREEL, Alexandre. Big Tech Acquisitions. 2020. Disponível em: https://cerre.eu/wp-content/uploads/2020/03/cerre_big_tech_acquisitions_2020.pdf Acessado em: 27/08/2021.

BRASIL. Marco Civil da Internet (Lei 12.965, 2014). Brasília, DF, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/Lei/l12965.htm Acessado em: 29/08/2021.

____. Constituição Federal. Brasília, DF, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm Acessado em: 29/08/2021.

____. Decreto-Lei 10.332. Institui a Estratégia de Governo Digital para o período de 2020 a 2022, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional e dá outras providências. Diário Oficial: seção 1, Brasília, DF, ano 156, nº 81, p. 01, 29 de abril de 2020. Disponível em: https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=29/04/2020&jornal=515&pagina=6&totalArquivos=61 Acessado em 22/05/2022.

____. Decreto-Lei 2.848. Institui o Código Penal Brasileiro. 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-Lei/del2848.htm Acessado em: 18/08/2022.

____. Câmara dos Deputados. **Projeto de Lei nº 7131, de 14 de abril de 2010**. Dispõe sobre a responsabilidade dos proprietários e autores de blogues e mecanismos similares. Brasília: Câmara dos Deputados, 2010. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=755059 Acesso em: 01/07/2023.

____. Câmara dos Deputados. **Projeto de Lei nº 4565, de 17 de outubro de 2012**. Modifica a Lei nº 8.078, de 11 de setembro de 1990, estabelecendo condições adicionais à contratação de provedores de aplicações na internet. Brasília: Câmara dos Deputados, 2012. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1031468 Acesso em: 01/07/2023.

____. Câmara dos Deputados. **Projeto de Lei nº 5596, de 16 de maio de 2013**. Proíbe o uso de aplicativos e redes sociais na internet para alertar motoristas sobre a ocorrência de blitz de trânsito. Brasília: Câmara dos Deputados, 2013. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1089377 Acesso em: 01/07/2023.

____. Câmara dos Deputados. **Projeto de Lei nº 2498, de 11 de agosto de 2015**. Acrescenta artigos à Lei nº 12.965, de 23 de abril de 2014, para obrigar os provedores de conexão e os provedores de aplicação de internet a criarem centros de atenção aos usuários compulsivos de serviços de internet e de redes sociais. Brasília: Câmara dos Deputados, 2015. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1366540&filename=PL%202498/2015 Acesso em: 01/07/2023.

____. Câmara dos Deputados. **Projeto de Lei nº 7460, de 24 de abril de 2017**. Altera a Lei nº 12.965, de 23 de abril de 2014, para obrigar provedores de aplicações de internet a retirarem conteúdos que promovam lesão contra a própria pessoa, automutilação, exposição à situação de risco de vida ou tentativa de suicídio, e a Lei nº 8.069, de 13 de julho de 1990, para tipificar o crime de indução à lesão contra a própria pessoa, automutilação, exposição à situação de risco de vida ou tentativa de suicídio, quando as vítimas forem crianças ou adolescentes. Brasília: Câmara dos Deputados, 2017. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1366540&filename=PL%202498/2015 Acesso em: 01/07/2023.

____. Câmara dos Deputados. **Projeto de Lei nº 77917, de 20 de junho de 2017**. Modifica o Marco Civil da Internet (Lei 12.965, 2014), instituído pela Lei no 12.965, de 23 de abril de 2014, dispondo sobre a publicação de mensagens de ajuda para o combate ao suicídio em aplicações de busca na internet. Brasília: Câmara dos Deputados, 2017. Disponível em:

https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1570720&filename=PL%207917/2017 Acesso em: 01/07/2023.

____. Câmara dos Deputados. **Projeto de Lei nº 10919, de 30 de outubro de 2018**. Obriga a identificação publicitária na exibição e na divulgação patrocinadas de produtos e serviços independente do meio de veiculação. Brasília: Câmara dos Deputados, 2018. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1689089&filename=PL%2010919/2018 Acesso em: 01/07/2023.

____. Câmara dos Deputados. **Projeto de Lei nº 2184 e 2185, de 09 de abril de 2019**. Acrescenta dispositivo à Lei nº 12.965, de 23 de abril de 2014, para obrigar os provedores de aplicações de redes sociais a veicularem campanhas informativas para evitar o compartilhamento e distribuição de imagens com nudez de crianças e adolescentes. Brasília: Câmara dos Deputados, 2019. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1730568&filename=PL%202185/2019 Acesso em: 01/07/2023.

____. Câmara dos Deputados. **Projeto de Lei nº 2463, de 23 de abril de 2019**. Dispõe sobre a limitação de divulgação de imagens e informações em veículos de mídia e redes sociais em situações de ataque massivo a pessoas. Brasília: Câmara dos Deputados, 2019. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1735938&filename=PL%202463/2019 Acesso em: 01/07/2023.

____. Câmara dos Deputados. **Projeto de Lei nº 3993, de 19 de julho de 2020**. Dispõe sobre a obrigatoriedade de apresentação de documentos comprobatórios da idade para acesso às plataformas digitais. Brasília: Câmara dos Deputados, 2020. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1917444&filename=PL%203993/2020 Acesso em: 01/07/2023.

____. Câmara dos Deputados. **Projeto de Lei nº 4120, de 07 de agosto de 2020**. Disciplina o uso de algoritmos pelas plataformas digitais na internet, assegurando transparência no uso das ferramentas computacionais que possam induzir a tomada de decisão ou atuar sobre as preferências dos usuários. Brasília: Câmara dos Deputados, 2020. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1921007&filename=PL%204120/2020 Acesso em: 01/07/2023.

____. Câmara dos Deputados. **Projeto de Lei nº 44801, de 02 de outubro de 2020**. Determina que as redes sociais insiram em suas plataformas alertas sobre o trabalho infantil e suas consequências. Brasília: Câmara dos Deputados, 2020. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1933929&filename=PL%204801/2020 Acesso em: 01/07/2023.

____. Câmara dos Deputados. **Projeto de Lei nº 5347, de 03 de dezembro de 2020**. Cria a Lei de Enfrentamento à Desinformação nas ELeições. Brasília: Câmara dos Deputados, 2020. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1945976&filename=PL%205347/2020 Acesso em: 01/07/2023.

____. Câmara dos Deputados. **Projeto de Lei nº 5567, de 17 de dezembro de 2020**. Estabelece obrigatoriedade as plataformas de mídias sociais para que instituam e mantenham mecanismos de controle de conteúdo. Brasília: Câmara dos Deputados, 2020. Disponível em:

https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1953329&filename=PL%205567/2020 Acesso em: 01/07/2023.

____. Câmara dos Deputados. **Projeto de Lei nº 2762, de 10 de agosto de 2021**. Altera a Lei nº 12.965, de 23 de abril de 2014, para obrigar provedores de aplicação de internet a instituírem mecanismos para alertar usuários sobre imagens humanas editadas digitalmente. Brasília: Câmara dos Deputados, 2021. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2054504&filename=PL%202762/2021 Acesso em: 01/07/2023.

____. Câmara dos Deputados. **Projeto de Lei nº 2831, de 16 de agosto de 2021**. Altera Altera o Marco Civil da Internet (Lei 12.965, 2014) - Lei nº 12.965, de 23 de abril de 2014 - para proibir a exclusão de postagens em redes sociais sem que se tenha concedido direito de ampla defesa e ao contraditório ao usuário responsável pela postagem, e dá outras providências. Brasília: Câmara dos Deputados, 2021. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2057399&filename=PL%202831/2021 Acesso em: 01/07/2023.

____. Câmara dos Deputados. **Projeto de Lei nº 3700, de 21 de outubro de 2021**. Altera a Lei no 12.965, de 23 de abril de 2014, para criar obrigações para os provedores de aplicação de internet na moderação de discursos de ódio. Brasília: Câmara dos Deputados, 2021. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2093192 Acesso em: 01/07/2023.

____. Câmara dos Deputados. **Projeto de Lei nº 188, de 09 de fevereiro de 2022**. Cria órgão no Ministério das Comunicações para fiscalizar veracidade nas mídias sociais. Brasília: Câmara dos Deputados, 2022. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2133872 Acesso em: 01/07/2023.

____. Câmara dos Deputados. **Projeto de Lei nº 630, de 18 de março de 2022**. Altera a Lei n. 12.965, de 23 de abril de 2014, para dispor sobre a necessidade de os provedores de redes sociais e de serviços de mensageria terem sede e representante legal radicado no país. Brasília: Câmara dos Deputados, 2022. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2150229 Acesso em: 01/07/2023.

____. Câmara dos Deputados. **Projeto de Lei nº 2557, de 04 de outubro de 2022**. Institui a Política Nacional de Proteção Digital das Crianças e Adolescentes – PNPD. Brasília: Câmara dos Deputados, 2022. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2208432 Acesso em: 01/07/2023.

____. Câmara dos Deputados. **Projeto de Lei nº 2768, de 10 de novembro de 2022**. Dispõe sobre a organização, o funcionamento e a operação das plataformas digitais que oferecem serviços ao público brasileiro e dá outras providências. Brasília: Câmara dos Deputados, 2022. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2214237&filename=PL%202768/2022 Acesso em: 01/07/2023.

____. Câmara dos Deputados. **Projeto de Lei nº 3046, de 20 de dezembro de 2022**. Altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet (Lei 12.965, 2014)), para disciplinar o procedimento relativo ao bloqueio de contas de membros do Congresso Nacional nas redes sociais da Internet. Brasília: Câmara dos Deputados, 2022. Disponível

em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2227370 Acesso em: 01/07/2023.

____. Senado Federal**. Projeto de Lei nº 347, de 19 de setembro de 2016.** Altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet (Lei 12.965, 2014)), para dispor sobre a necessidade de prévio consentimento do usuário nos processos de cadastramento e envio de convites para participação em redes e mídias sociais, bem como em seus respectivos grupos, páginas, comunidades e similares. Brasília: Senado Federal, 2016. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/126964 Acesso em: 01/07/2023.

____. Senado Federal**. Projeto de Lei nº 2630, de 13 de maio de 2020.** Institui a Lei BrasiLeira de Liberdade, Responsabilidade e Transparência na Internet. Brasília: Senado Federal, 2020. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/141944 Acesso em: 01/07/2023.

BREGA, Gabriel Ribeiro. A regulação de conteúdo nas redes sociais: uma breve análise comparativa entre o NetzDG e a solução brasileira. Revista Direito GV, v. 19, 2023. Disponível em: https://www.scielo.br/j/rdgv/a/qwwzmCyw5FmFQmTpRw3HCQh/abstract/?lang=pt Acessado em 11/04/23023.

BROERSMA, Marcel; ELDRIDGE II, Scott A. *Journalism, and social media: redistribution of power?* **Media and Communication**, v. 7, n. 1, p. 193-197, 2019. Disponível em: https://www.ssoar.info/ssoar/handle/document/61850 Acessado em: 28/08/2021.

BRIGGS, Asa; BURKE, Peter. **Uma história social da mídia: de Gutenberg à Internet.** Editora Schwarcz-Companhia das Letras, 2016.

BURGESS, Jean. *Platform studies*. In: **Creator culture: An introduction to global social media entertainment**, p. 21-38, 2021.

BURKE, Peter. **Uma história social do conhecimento 1: de Gutenberg a Diderot.** Editora Schwarcz-Companhia das Letras, 2003.

CABRERA, José Maria Léon. *How Google is suffocating independente journalism in Latin America*. **Columbia Journalism Review**, 27 feb. 2023.

CALLEJÓN, María Luisa Balaguer. Crónica de la legislación europea. Segundo semestre de 2022. **Revista de derecho constitucional europeo**, n. 38, p. 10, 2022. Disponível em: https://dialnet.unirioja.es/servlet/articulo?codigo=8793553 Acessado em: 11/11/2023.

CAMARGO, Aline; MAGNONI, Antonio Francisco; MIRANDA, Giovani Vieira. Comunicação Política, Internet, Juventude e Participação: proposta de reflexão. **Comunicação: Reflexões, experiências, ensino**, v. 14, n. 1, 2018.

CASTELLS, Manuel. **O poder da identidade**. Editora Paz e Terra, 2018.

CITRON, Danielle Keats; JURECIC, Quinta. *FOSTA's Mess.* **Virginia Public Law and Legal Theory Research Paper,** n. 62, 2022. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4204983 Acessado em: 20/06/2023.

CHATILA, Raja *et al. The IEEE global initiative for ethical considerations in artificial intelligence and autonomous systems* [standards]. **IEEE Robotics & Automation Magazine**, v. 24, n. 1, p. 110-110, 2017.

COMPETITION, Australian *et al.* ACCC/OAIC compliance and enforcement policy for the Consumer Data Right. 2020.

CONNOLLY, Chris; DIJK, Peter van. *Enforcement and Reform of the EU-US Safe Harbor Agreement*. In: **Enforcing Privacy**. Springer, Cham, 2016. p. 261-283.

CORRENTI, Antonella. *Online platforms as a complex digital environment characterised by a lack of transparency on the role and status of the parties involved, as well as the use of unfair commercial practices*. **European Journal of Privacy Law & Technologies**, n. 2, 2022.

COZZOLINO, Alessio; CORBO, Leonardo; AVERSA, Paolo. *Digital platform-based ecosystems: The evolution of collaboration and competition between incumbent producers and entrant platforms*. **Journal of Business Research**, v. 126, p. 385-400, 2021. Disponível em: https://www.sciencedirect.com/science/article/pii/S0148296320308894 Acessado em: 16/04/2021.

COULDRY, Nick; MEJIAS, Ulises A. *The costs of connection*. In: The Costs of Connection. Stanford University Press, 2019.

CURZI, Yasmin *et al.* **Nota técnica do Centro de Tecnologia e Sociedade da FGV Direito Rio sobre o substitutivo ao PL 2630/2020**. 2021. Disponível em: https://bibliotecadigital.fgv.br/dspace/handle/10438/31348 Acessado em: 01/05/2023.

CUSUMANO, Michael A.; GAWER, Annabelle; YOFFIE, David B. *Can self-regulation save digital platforms?.* **Industrial and Corporate Change**, v. 30, n. 5, p. 1259-1285, 2021.

DAGOULA, Chrysi. *Mapping political discussions on Twitter: Where the elites remain elites.* **Media and Communication**, v. 7, n. 1, p. 225-234, 2019. Disponível em: https://www.cogitatiopress.com/mediaandcommunication/article/view/1764 Acessado em 28/08/2021.

DATASENADO. Mais de 80% dos brasiLeitos acreditam que redes sociais influenciam muito a opinião das pessoas. Senado Federal. 2019. Disponível em: https://www12.senado.leg.br/institucional/datasenado/materias/pesquisas/mais-de-80-dos-brasiLeiros-acreditam-que-redes-sociais-influenciam-muito-a-opiniao-das-pessoas Acessado em: 15/03/2022.

DE CASTRIS, Arcangelo Leone. **Types of Platform Transparency: An analysis of digital platforms and policymakers discourse on Big Tech governance and transparency**. 2022. Tese de Doutorado. UNIVERSITY OF CHICAGO. Disponível em: file:///C:/Users/PC/Downloads/Leone%20de%20Castris_Arcangelo_MAPSS%20Thesis.pdf Acessado: 23/06/2023.

DE ALMEIDA, Rosana Santos *et al.* A liberdade de expressão e seus limites: uma análise crítica do Marco Civil da Internet (Lei 12.965, 2014). **Research, Society and Development**, v. 11, n. 2, p. e39111225445-e39111225445, 2022. Disponível em: https://rsdjournal.org/index.php/rsd/article/view/25445 Acessado em 01/05/2023.

DE LIMA, Marcos Francisco Urupá Moraes *et al.* Regulação de plataformas digitais: mapeando o debate internacional. **Liinc em Revista**, v. 16, n. 1, p. e5100-e5100, 2020. Disponível Acessado em: 31/05/21.

DE TERWANGNE, Cécile. *Article 5 principles relating to processing of personal data*. In: **The EU general data protection regulation (GDPR)**. Oxford University Press, 2020.

DELACEY, Hannah. *A Critical Analysis of the Enactment of the Allow States and Victims to Fight Online Sex Trafficking Act of 2018*. **International Journal of Gender, Sexuality and Law**, v. 2, n. 1, p. 100-139, 2022. Disponível em: https://journals.northumbria.ac.uk/index.php/IJGSL/article/view/1257 Acessado em: 20/06/2023.

DI FELICE, Massimo. **A Cidadania Digital: A crise da ideia ocidental de democracia e a participação nas redes digitais.** Paulus Editora, 2021.

DI NICOLA, Andrea. *Towards digital organized crime and digital sociology of organized crime.* **Trends in organized crime**, p. 1-20, 2022. Disponível em: https://link.springer.com/article/10.1007/s12117-022-09457-y Acessado: 26/06/2023.

DOS SANTOS, Bruna Martins. Uma avaliação do Modelo de Responsabilidade de Intermediários do Marco Civil para o desenvolvimento da Internet no Brasil. **Internet Society, Capítulo Brasil.** 2020. Disponível em: https://isoc.org.br/files/1_5163560127365644511.pdf Acessado em: 01/05/2023.

DOUGLAS, Erika. *Constructing the Digital Regulatory Ecosystem: Agency Collaboration*. **Virginia Journal of Law and Technology**, v. 26, n. 1, 2023. Disponível em: file:///C:/Users/PC/Downloads/SSRN-id4408318.pdf Acessado em: 23/06/2023.

EDWARDS, Jan; LANE, Rick. *Three Kids' Internet Safety Bills You Need to Know.* [Entrevista concedida a Lynn Shaw]. **Lynn's Warriors**, 16 set. 2022. Disponível em: https://www.youtube.com/watch?v=5bSuNfjqWNc Acessado em: 13/06/2023.

EUROPEU, Parlamento; DA UNIÃO EUROPEIA, Conselho. Directiva 2010/13/UE-Directiva «Serviços de Comunicação Social Audiovisuall. **Retirado de http://www. gmcs. pt/pt/directiva-201013ue-directiva-servicos-de-comunicacao-socialaudiovisual**, 2008.

EUROPEU, Parlamento; CONSELHO, DA UNIÃO EUROPEIA. Regulamento (UE) 2016/679. **Regulamento Geral de Proteção de Dados da União Europeia** de, v. 27, 2016.

EUROPEU, Parlamento; DA UNIÃO EUROPEIA, Conselho. Diretiva (UE) 2018/1808 do Parlamento Europeu e do Conselho, de 14 de novembro de 2018. **Diario Oficial de la Unión Europea**, 2018.

EUROPEU, Parlamento; CONSELHO, DA UNIÃO EUROPEIA. Regulamento (UE) 2019/1150. Regulamento relativo à promoção da equidade e da transparência para os utilizadores profissionais de serviços de intermediação em linha **Jornal Oficial da União Europeia,** Luxemburgo, n. 186, p. 57-79, 2019.

EUROPEU, Parlamento; CONSELHO, DA UNIÃO EUROPEIA. Regulamento (UE) 2021/784. Regulamento relativo ao combate à difusão de conteúdos terroristas em linha **Jornal Oficial da União Europeia,** Luxemburgo, n. 172, p. 79-109, 2021.

EUROPEU, Parlamento; CONSELHO, DA UNIÃO EUROPEIA. Regulamento (UE) 2022/991. Regulamento que altera o Regulamento (UE) 2016/794 no que diz respeito à cooperação da Europol com os organismos privados, ao tratamento de dados pessoais pela Europol para apoiar investigações criminais, e ao papel da Europol na investigação e inovação. **Jornal Oficial da União Europeia,** Luxemburgo, n. 169, p. 1-42, 2022.

EUROPEU, Parlamento; CONSELHO, DA UNIÃO EUROPEIA. Regulamento (UE) 2022/1925. Regulamento relativo à disputabilidade e equidade dos mercados no setor digital e que altera as Diretivas (UE) 2019/1937 e (UE) 2020/1828 (Regulamento dos Mercados Digitais). **Jornal Oficial da União Europeia,** Luxemburgo, n. 265, p. 1-66, 2022.

EUROPEU, Parlamento; CONSELHO, DA UNIÃO EUROPEIA. Regulamento (UE) 2022/2065. Regulamento relativo a um mercado único para os serviços digitais e que altera a Diretiva 2000/31/CE (Regulamento dos Serviços Digitais) **Jornal Oficial da União Europeia,** Luxemburgo, n. 277, p. 1-102, 2022.

EUROPEU, Parlamento; CONSELHO, DA UNIÃO EUROPEIA. Diretiva (UE) 2022/2555. Diretiva relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União que altera o Regulamento (UE) n.o 910/2014 e a Diretiva (UE) 2018/1972 e revoga a Diretiva (UE) 2016/1148 (Diretiva SRI 2). **Jornal Oficial da União Europeia,** Luxemburgo, n. 333, p. 80-152, 2022.

FACEBOOK. Who We Are. 2021. Disponível em:Acessado em: 06/07/2021.

FELD, Harold. *The Case for the Digital Platform Act*. **PdF YouTube**, 28 de jun. 2019. Disponível em: https://www.youtube.com/watch?v=UyRQLmKZQAA&t=82s Acessado: 23/06/2023.

FILGUEIRAS, Vitor; ANTUNES, Ricardo. Plataformas digitais, Uberização do trabalho e regulação no Capitalismo contemporâneo. **Revista Contracampo**, v. 39, n. 1, 2020. Disponível em: https://periodicos.uff.br/contracampo/article/view/38901 Acessado em: 01/06/2021.

FINCK, Michèle. *Digital co-regulation: designing a supranational legal framework for the platform economy*. **European Law Review**, 2018.

FLEW, Terry; MARTIN, Fiona; SUZOR, Nicolas. *Internet regulation as media policy: Rethinking the question of digital communication platform governance*. **Journal of Digital Media & Policy**, v. 10, n. 1, p. 33-50, 2019. Disponível em: Acessado em: 27/05/21.

FLEW, Terry. *Platforms on trial*. **Intermedia**, v. 46, n. 2, p. 24-29, 2018. Disponível e Acessado em: 28/05/21.

FINKELSTEIN, Maria Eugenia; FINKELSTEIN, Claudio. Privacidade e Lei geral de proteção de dados pessoais. **Revista de Direito BrasiLeira**, v. 23, n. 9, p. 284-301, 2020.

FORNASIER, Mateus de Oliveira; KNEBEL, Norberto Milton Paiva. O titular de dados como sujeito de direito no capitalismo de vigilância e mercantilização dos dados na Lei Geral de Proteção de Dados. **Revista Direito e Práxis**, v. 12, p. 1002-1033, 2021. Disponível em: https://www.scielo.br/j/rdp/a/hTqmGJVy7FP5PWq4Z7RsbCG/?format=html&lang=pt Acessado em 01/05/2023.

FRANCO, David Silva; FERRAZ, Deise Luiza da Silva. Uberização do trabalho e acumulação capitalista. **Cadernos EBAPE. BR**, v. 17, p. 844-856, 2019. Disponível em: https://www.scielo.br/j/cebape/a/9NJd8xMhZD3qJVwqsG4WV3c/abstract/?lang=pt Acessado em: 26/08/2021.

FUCHS, Christian. *The digital commons and the digital public sphere: How to advance digital democracy today.* **Westminster Papers in Communication and Culture**, v. 16, n. 1, 2021. Disponível em: https://www.westminsterpapers.org/article/id/917/ Acessado em: 11/08/2021.

GEIGER, Christophe *et al.* Os artilheiros que estão faltando no time da inteligência artificial: Big Data, o direito fundamental à pesquisa, e as (insuficientes) limitações para mineração de textos e dados na Diretiva (UE) 2019/790 relativa aos direitos de autor no mercado único digital. **INTERNET&SOCIEDADE**, v. 3, n. 2, p. 108-121, 2022. Disponível em: https://iris.luiss.it/bitstream/11385/225478/1/CHF985~1.PDF Acessado em: 11/11/2023.

GELLIS, Cathy. What is the NUDGE Act? [Entrevista concedida a Leo Laporte, Jeff Jarvis, Ant Pruitt]. TWiT **Tech Podcast Network**, 16 fev. 2022. Disponível em: https://twit.tv/shows/this-week-in-google/episodes/651 Acessado em: 07/06/2023.

GILLESPIE, Tarleton. Do not recommend reduction thecniques, as a form of moderation. **DIMACS CCICADA**, 27 mai. 2022. Disponível em: https://www.youtube.com/watch?v=WZbI9L7AfXM Acessado em 23/08/2022.

GILLESPIE, Tarleton. How platforms reduce visibility of some content. **Digital Society**, 16 dez. 2021. Disponível em: https://www.youtube.com/watch?v=a-CZpIIKaco Acessado em 23/08/2022.

GILLESPIE, Tarleton. ***Custodians of the Internet***. Yale University Press, 2018.

GILLESPIE, Tarleton. *Platforms are not intermediaries.* **Georgetown Law Technology Review**, v. 2, n. 2, p. 198-216, 2018b. Disponível em: Acesso em: 02/06/21

GORWA, Robert; ASH, Timothy Garton. *Democratic transparency in the platform society*. **Social Media and Democracy: The State of the Field, Prospects for Reform**, p. 286, 2020.

GORWA, Robert; BINNS, Reuben; KATZENBACH, Christian. *Algorithmic content moderation: Technical and political challenges in the automation of platform governance*. **Big Data & Society**, v. 7, n. 1, p. 2053951719897945, 2020.

GORWA, Robert. Giganet annual symposium – room a panel 1 – platform governance. Giganet, 2020. Disponível em: https://www.youtube.com/watch?v=TQTPFNAT9pk Acessado em 23/08/2022.

GORWA, Robert. *The platform governance triangle: Conceptualising the informal regulation of online content*. **Internet Policy Review**, v. 8, n. 2, p. 1-22, 2019.

GRIMMELMANN, James. *The virtues of moderation*. **Yale JL & Tech**., v. 17, p. 42, 2015.

GROHMANN, Rafael. Plataformização do trabalho: entre dataficação, financeirização e racionalidade neoliberal. **Revista Eletrônica Internacional de Economia Política da Informação, da Comunicação e da Cultura**, v. 22, n. 1, p. 106-122, 2020. Disponível em: https://seer.ufs.br/index.php/eptic/article/view/12188/10214 Acessado em: 10/08/2021.

HARCUP, Tony; O'NEILL, Deirdre. *What is news? News values revisited (again).* **Journalism studies,** v. 18, n. 12, p. 1470-1488, 2017. Disponível em: https://www.tandfonline.com/doi/full/10.1080/1461670X.2016.1150193 Acessado em: 01/05/2020.

HELBERGER, Natali; PIERSON, Jo; POELL, Thomas. *Governing online platforms: From contested to cooperative responsibility.* **The information society**, v. 34, n. 1, p. 1-14, 2018.

HELBING, Dirk *et al. Will democracy survive big data and artificial intelligence?.* In: **Towards digital enlightenment**. Springer, Cham, 2019. p. 73-98.

HIREMATH, B. K.; KENCHAKKANAVAR, Anand Y. An alteration of the web 1.0, web 2.0 and web 3.0: a comparative study. **Imperial Journal of Interdisciplinary Research**, v. 2, n. 4, p. 705-710, 2016.

HOGAN, Bernie. *Social media giveth, social media taketh away: Facebook, friendships, and APIs*. **International Journal of Communication**, Forthcoming, 2016.

HOUSE, Freedom. Freedom on the Net 2021-United Kingdom. 2021.

INTERNACIONAL COMMUNICATION UNION. Global Connectivity Report. 2022. Disponível em: Acessado em 25/07/2022.

INTERVOZES. **Padrões para uma regulação democrática das grandes plataformas.** São Paulo: 2020. Disponível em:https://intervozes.org.br/publicacoes/padroes-para-uma-regulacao-democratica-das-grandes-plataformas-que-garanta-a-liberdade-de-expressao-online-e-uma-internet-livre-e-aberta/ Acessado em 13/01/2024.

ISABELLE, Diane *et al. The role of analytics in data-driven business models of multi-sided platforms: An exploration in the food industry*. **USN Open Archives**, 2020. Disponível em: https://openarchive.usn.no/usn-xmlui/handle/11250/2736679 Acessado em: 29/08/2021.

JANOWSKI, Tomasz; ESTEVEZ, Elsa; BAGUMA, Rehema. *Platform governance for sustainable development: Reshaping citizen-administration relationships in the digital age*. **Government Information Quarterly**, v. 35, n. 4, p. S1-S16, 2018.

JENKINS, Henry; FORD, Sam; GREEN, Joshua. **Cultura da conexão: criando valor e significado por meio da mídia propagável**. Aleph, 2015.

JIMÉNEZ DURÁN, Rafael. *The economics of content moderation: Theory and experimental evidence from hate speech on Twitter*. **Available at SSRN**, 2022.

JOHNSTON, Jane; WALLACE, Anne. Law Defining Journalists: Who's who in the age of digital media?. In: **The Routledge Handbook of Developments in Digital Journalism Studies.** Routledge, 2018. p. 15-27. Disponível em: https://www.taylorfrancis.com/chapters/edit/10.4324/9781315270449-2/law-defining-journalists-jane-johnston-anne-wallace Acessado em: 28/08/2021.

KARHAWI, Issaaf. Crises geradas por influenciadores digitais: propostas para prevenção e gestão de crises. **Organicom**, v. 18, n. 35, p. 45-59, 2021. Disponível em: https://www.revistas.usp.br/organicom/article/view/172213 Acessado em: 25/08/2021.

KAYSER-BRIL, Nicolas. *At least 11 police forces use face recognition in the EU***. AlgorithmWatch.** 2021.

KELLER, Daphne. *Testimony and Follow-Up Responses, United States Senate Committee on the Judiciary, Subcommittee on Intellectual Property Hearing on the Digital Millennium Copyright Act at 22: How Other Countries Are Handling Online Piracy*. **United States Senate Committee on the Judiciary, Subcommittee on Intellectual Property Hearing on the Digital Millennium Copyright Act at**, v. 22, 2020a.

_____. Daphne Keller of the Stanford Cyber Policy Center on "Who Controls Online Speech?". **UCLA School of Law,** 22 abr. 2020b. Disponível em: https://www.youtube.com/watch?v=vhyeJ2RelJI Acessado em 18/09/2022.

_____. Social Media and Democracy. Stanford Ciber Policy Center, 8 set. 2020c. Disponível em: https://www.youtube.com/watch?v=vhyeJ2RelJI Acessado em 22/08/2022.

_____. Amplification and its discontents. **Knight First Amendment Institute**, v. 8, 2021. Disponível em: https://knightcolumbia.org/content/amplification-and-its-discontents Acessado em 22/08/2022.

KOENIG, Brett *et al. Digital Exclusion and the Structural Barriers to Safety Strategies among Men and Non-Binary Sex Workers Who Solicit Clients Online.* **Social Sciences**, v. 11, n. 7, p. 318, 2022. Disponível em: https://www.mdpi.com/2076-0760/11/7/318 Acessado em: 21/06/2023.

KNOCHE, Manfred. *Capitalisation of the Media Industry From a Political Economy Perspective*. **tripleC: Communication, Capitalism & Critique. Open Access Journal for a Global Sustainable Information Society**, v. 19, n. 2, p. 325-342, 2021. Disponível em: https://www.triple-c.at/index.php/tripleC/article/view/1283 Acessado em: 27/08/2021.

KONOPACKI, Marco; GETSCHKO, Demi. Marco Civil da Internet (Lei 12.965, 2014). [Entrevista concedida a Cristiano Reckziegel]. **Conexão Futura**, 31 mai. 2016. Disponível em: https://www.youtube.com/watch?v=m2Hb6YbGkyo Acessado em: 02/06/2023.

KOZLOWSKA, Iga. *Facebook and data privacy in the age of Cambridge Analytica*. **The Henry M. Jackson School of International Studies**, Seatlle, v. 30, 2018.

KUNER, Christopher; BYGRAVE, Lee A.; DOCKSEY, Christopher. *Background and Evolution of the EU General Data Protection Regulation (GDPR)*. In: **The EU General Data Protection Regulation (GDPR)**. Oxford University Press, 2020.

KUENZLER, Adrian. *On (some aspects of) social privacy in the social media space*. **International Data Privacy Law**, v. 12, n. 1, p. 63-73, 2022.

LIGHT, Evan; OBAR, Jonathan A. *Surveillance reform: revealing surveillance harms and engaging reform tactics*. In: **Research Handbook on Human Rights and Digital Technology**. Edward Elgar Publishing, 2019.

LOLLINI, Massimo; FARLEY, Arthur; LÈVY, Pierre. Collective Intelligence, the Future of Internet and the IEML. **Humanist Studies & the Digital Age**, v. 6, n. 1, p. 5-31, 2019.
LUMEN. About us. 2022 Disponível em: https://www.lumendatabase.org/pages/about Acessado em: 14/09/2022.

LOWRY, Samuel. *Social media and foreign influence on intelligence.* **Harvard Model Congress**, 2020. Disponível em: https://static1.squarespace.com/static/5cb7e5637d0c9145fa68863e/t/5e40e592ff19c478903e8513/1581311378237/Lowry_HomelandBriefingUpdate_SocialMediaandForeignInfluenceonIntelligence.pdf Acessado em: 17/06/2023.

MACKENZIE-GRAY SCOTT, Richard. *Managing Misinformation on Social Media: Targeted Newsfeed Interventions and Freedom of Thought*. **Northwestern Journal of Human Rights**, v. 21, n. 2, p. 109, 2023. Disponível em: https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1251&context=njihr Acessado em: 07/06/2023.

MALYSHEV, Nick; KAUFFMANN, C. ***Regulatory effectiveness in the era of digitalisation.*** 2019.

MANOVICH, Lev. Digital traces in context| 100 billion data rows per second: Media analytics in the early 21st century. **International journal of communication,** v. 12, p. 16, 2018.

MANSELL, Robin; STEINMUELLER, W. EDWARD. *Denaturalizing digital platforms: is mass individualization here to stay?*. **International Journal of Communication**, 2020.

MARANHÃO, Juliano; CAMPOS, Ricardo; GUEDES, Jéssica; OLIVEIRA, Samuel Rodrigues de; GRINGS, Maria Gabriela. **Regulação de "Fake News" no Brasil**. São Paulo: Instituto Legal Grounds, 2021. Disponível em: https://institutoLGPDcom/wp-content/uploads/2021/10/Regulacao-de-FAKE-NEWS-no-Brasil_impressao.pdf Acessado em 03/06/2023.

MARKEY, Edward; MURTHY, Vivek. *Addressing the Youth Mental Health Crisis*. 5 jun. 2023. [Entrevista concedida a Sandro Galea] **Boston University School of Public Health.** Disponível em: https://www.youtube.com/watch?v=6EnmRqEmyoU Acessado: 15/06/2023.

MARTINS, Jorge Silva. Factos e mitos sobre o RGPD / LGPD - Portugal. **E-Commerce Experience**. 22 nov. 2019. Disponível em: https://www.youtube.com/watch?v=in39ZdE4U64 Acessado em 04/11/2023.

MCCHESNEY, Robert W. ***Rich media, poor democracy: Communication politics in dubious times.*** New Press, The, 2016.

MCCRACKEN, Harry; HOWELL, Denise; THOMSON, Iain. *Craigslist Personals Shut Down Due to SESTA/FOSTA*. [Entrevista concedida a Leo Laporte]. **TWiT Tech Podcast Network**, 26 mar. 2018. Disponível em: https://www.youtube.com/watch?v=FO_xBuhh24E Acessado em: 21/06/2023.

MCDERMOTT, Meghan E. *Mitigating Misinformation on Social Media Platforms: Treating Section 230 of the Communications Decency Act as a Quid Pro Quo Benefit*. **Conn. L. Rev. Online**, v. 55, p. 1, 2023. Disponível em: https://heinonline.org/HOL/LandingPage?handle=hein.journals/conntemp55&div=4&id=&page= Acessado em: 01/05/2023.

MINTZ, André Goes. Midiatização e plataformização: aproximações. **Novos Olhares**, v. 8, n. 2, p. 98-109, 2019. Disponível e Acessado em: 28/05/21.

MONEA, Alexander. **The digital closet.** MIT Press, 2022.

MOROZOV, Evgeny. **Big tech**. Ubu Editora LTDA-ME, 2018.

MYERS WEST, Sarah. *Censored, suspended, shadowbanned: User interpretations of content moderation on social media platforms*. **New Media & Society**, v. 20, n. 11, p. 4366-4383, 2018.

NAPOLITANO, Carlo José; RANZANI, Luiz Henrique. Regulação democrática de plataformas de rede social: possibilidades da autorregulação regulada no Brasil. **Revista Eletrônica Internacional de Economia Política da Informação da Comunicação e da Cultura**, v. 23, n. 3, p. 183-199, 2021.
Disponível em: https://ufs.emnuvens.com.br/eptic/article/view/16332/12389 Acessado em: 24/02/2024.

NIEBORG, David B.; POELL, Thomas. *The platformization of cultural production: Theorizing the contingent cultural commodity*. **New media & society**, v. 20, n. 11, p. 4275-4292, 2018. Disponível em Acessado em 01/06/21.

ONYEAGBAKO, Victoria; ADEYOJU, Ademola. *Revisiting Data Protection, Privacy and State Surveillance*. **Privacy and State Surveillance** (February 18, 2021), 2021.

OROFINO, Marco *et al. La normativa a tutela dei minori nel Testo Unico per la fornitura di servizi di media audiovisivi con uno sguardo rivolto al Regolamento UE 2022/2065*. **MEDIA LAWS**, v. 2022, n. 3, p. 1-17, 2022. Disponível em: https://air.unimi.it/handle/2434/954475 Acessado em: 11/11/2023.

OTERO, Juan María Martínez. *Un nuevo marco regulador para el sector audiovisual en Europa: la Directiva 2018/1808 en el contexto de la convergencia mediática y el Mercado Único Digital*. **Revista de Derecho Comunitario Europeo**, v. 23, n. 63, p. 537-571, 2019. Disponível em: https://dialnet.unirioja.es/servlet/articulo?codigo=7014954 Acessado em: 01/11/2023.

PADOVANI, Claudia. *Debating communication imbalances from the MacBride Report to the World Summit on the Information Society: An analysis of a changing discourse.* **Global Media and Communication**, v. 1, n. 3, p. 316-338, 2005. Disponível em: https://www.researchgate.net/publication/258138117 Acessado em: 21/09/2020.

PAGOTO, Sherry *et al. A call for a public health agenda for social media research*. **Journal of medical Internet research**, v. 21, n. 12, p. e16661, 2019. Disponível em: https://www.jmir.org/2019/12/e16661 Acessado em 16/06/2023.

PALLERO, *et al.* Padrões para uma regulação democrática das grandes plataformas. 2020. Disponível em: https://idec.org.br/sites/default/files/padroes_para_uma_regulacao_democratica_das_grandes_plataformas_final.pdf Acessado em: 08/04/2023.

PAPAEVANGELOU, Charis. *Funding Intermediaries: Google and Facebook's Strategy to Capture Journalism. Digital Journalism*, p. 1-22, 2022. Disponível em: https://shs.hal.science/halshs-03748885/document Acessado em 08/04/2023.

PARK, Hyun Jung; LIN, Li Min. *The effects of match-ups on the consumer attitudes toward internet celebrities and their live streaming contents in the context of product endorsement.* **Journal of Retailing and Consumer Services**, v. 52, p. 101934, 2020. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0969698918309962 Acessado em: 29/08/2021.

PARKER, Geoffrey; PETROPOULOS, Georgios; VAN ALSTYNE, Marshall W. *Digital platforms and antitrust*. **Available at SSRN 3608397**, 2020. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3608397 Acessado em 29/08/2021.

PFEFFERKORN, Riana. *The EARN IT Act Is Back, and It's More Dangerous than Ever.* **Center for Internet and Society,** 2022. Disponível em: https://cyberlaw.stanford.edu/blog/2022/02/earn-it-act-back-and-it%E2%80%99s-more-dangerous-ever Acessado em: 20/06/2023.

PICARD, Robert; PICKARD, Victor. ***Essential principles for contemporary media and communications policymaking***. 2017.

PIERRE LÈVY. **Cibercultura**. Editora 34, 2010.

PINHEIRO, Alexandre Pereira; PINHEIRO, Guilherme. Buscadores e Redes Sociais: Limites da Moderação e da Liberdade Editorial dos Provedores de Aplicações na Internet. **REI-REVISTA ESTUDOS INSTITUCIONAIS**, v. 7, n. 2, p. 588-605, 2021.

POELL, Thomas; NIEBORG, David; VAN DIJCK, José. Plataformização. **Fronteiras-estudos midiáticos**, v. 22, n. 1, p. 2-10, 2020. Disponível em: Acessado em 01/06/21.

POLETTO, Álerton Emanuel; DE MORAIS, Fausto Santos. A moderação de conteúdo em massa por plataformas privadas de redes sociais. **Prisma Juridico**, v. 21, n. 1, p. 108-126, 2022.

PRABHU, Trisha. *Social media and foreign influence on intelligence*. **Harvard Model Congress**. Boston. 2020. Disponível em: https://static1.squarespace.com/static/5cb7e5637d0c9145fa68863e/t/5dddc3e00c91bc6c3b6c30c0/1574814688403/Senate_Homeland_3.pdf Acessado em: 17/06/2023.

RAMOS, Armando Dias. A IA e a sua aplicação na investigação criminal: contributo para a identificação de perfis na criminalidade organizada. **Anatomia do Crime**, v. 17, n. Jan-Jun, p. 159-168, 2023. Disponível em: file:///C:/Users/PC/Downloads/87667-a-ia-e-a-sua-aplicacao-na-investigacao-criminal-contributo-para-a-identificacao-de-perfis-na-criminalidade-organizada.pdf Acessado em: 11/11/2023.

RANKING DIGITAL RIGHTS. Who we are. Disponível em: https://rankingdigitalrights.org/who-we-are/ Acessado em 19/05/2022.

RIBEIRO, Marcia Carla Pereira; HERBST, Kharen Keim. Direitos Autorais no Blockchain: Escassez como Incentivo para Produção ou Concentração de Riqueza?. **Economic Analysis of Law Review**, v. 11, n. 3, p. 16-27, 2020. Disponível em: https://www.proquest.com/openview/45862c391b8bdd74bec9e8e9697217b8/1?pq-origsite=gscholar&cbl=1226335 Acessado em: 30/08/2021.

RIBEIRO-NAVARRETE, Samuel; SAURA, Jose Ramon; PALACIOS-MARQUÉS, Daniel. *Towards a new era of mass data collection: Assessing pandemic surveillance technologies to preserve user privacy*. **Technological Forecasting and Social Change**, v. 167, p. 120681, 2021.

RONZHYN, Alexander; WIMMER, Maria A. *Literature review of ethical concerns in the use of disruptive technologies in government 3.0*. In: **Icds.** 2019. p. 85-93.

RÜDIGER, Francisco. As redes e a armação: Da cultura do narcisismo ao fetichismo tecnológico. **Comunicação, Cultura e Mídias Sociais,** 2016. Disponível em: https://repositorio.pucrs.br/dspace/bitstream/10923/9959/2/As_redes_e_a_armacao_Da_cultura_do_narcisismo_ao_fetichismo_tecnologico.pdf Acessado em: 01/08/2021.

RUEDIGER, Marco Aurelio *et al.* Regulação de plataformas digitais: uma contribuição para a análise do debate nacional frente a um desafio global: **FGV DAPP**, 2022. Disponível em: https://democraciadigital.dapp.fgv.br/wp-content/uploads/2022/05/PTEstudo-8_FichaISBN.pdf Acessado em: 08/04/2023.

RUIJER, Erna *et al. Open data work: understanding open data usage from a practice lens*. **International Review of Administrative Sciences**, v. 86, n. 1, p. 3-19, 2020.

RUIZ DÍAZ, Lucas J. The European Parliament's Oversight of the Agencies of the Area of Freedom, Security and Justice. Where are we Now and Where are we Heading. **Cuadernos Europeos de Deusto**, v. 67 p. 29-59, 2022.

SAPONE, Larissa. *Moving Fast & Breaking Things: An Analysis of Social Media's Revolutionary Effects on Culture and Its Impending Regulation*. **Duquesne Law Review**, v. 59, n. 2, p. 362, 2021. Disponível em: https://dsc.duq.edu/cgi/viewcontent.cgi?article=3918&context=dlr Acessado em: 16/06/2023.

SCHUMER, Chuck *et al.* RE: *Fourth Amendment Issues Posed by the EARN IT Act* (S. 1207, HR 2732). 2023. Disponível em: https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=3781&context=historical Acessado em: 20/06/2023.

SEMICEK, Paulo Henrique; BOTELHO-FRANCISCO, Rodrigo Eduardo; DE LIMA, Myrian Regina del Vecchio. "This is your digital life": redes, mídias sociais e o impacto do caso Cambridge Analytica na Política de Dados do Facebook. **Fronteiras-estudos midiáticos**, v. 23, n. 3, 2021.

SÊMOLA, Marcos; BLUM, Renato Opice. Os impactos da LGPD. [Entrevista concedida a Laura Ignacio]. **Valor Econômico**, 10 ago. 2021. Disponível em: https://www.youtube.com/watch?v=cTO3zRNf6Qo Acessado em: 02/06/2023.

SERRANÍA, Vanessa Jiménez; ABRUSIO, Juliana. BIG DATA E A COMPETIÇÃO BASEADA EM DADOS. **Revista de Direito BrasiLeira**, v. 28, n. 11, p. 387-404, 2021.Disponível em: https://www.indexlaw.org/index.php/rdb/article/view/6819 Acessado em: 11/11/2023.

SILVA, Alexandre Pacheco da *et al.* Reformas do Direito do Autor na Era Digital-Resultados Preliminares de Pesquisa. 2021.

SILVA, Luiz Rogério Lopes *et al.* A gestão do discurso de ódio nas plataformas de mídias sociais digitais: um comparativo entre Facebook, Twitter e Youtube. **Revista ibero-americana de ciência da informação**, v. 12, n. 2, p. 470-492, 2019.

SPENCER, Shaun B. *The First Amendment and the Regulation of Speech Intermediaries*. **Marquette Law Review**, Forthcoming, 2022. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4132690 Acessado em: 01/05/2023.

STEEVES, Valerie; MAČĖNAITĖ, Milda. *Data protection and childrens online privacy.* In: **Research Handbook on Privacy and Data Protection Law.** Edward Elgar Publishing, 2022. p. 358-374.

STEPANOVICH, A.; MITNIC, D. *Universal implementation guide for the international principles on the application of human rights to communications surveillance*. AccessNow. 2015.

SUZOR, Nicolas; GILLETT, Rosalie. *Self-regulation and Discretion.* In: **Digital Platform Regulation: Global Perspectives on Internet Governance.** Cham: Springer International Publishing, 2022. p. 259-279.

SWORDS, Jon; LAING, Mary; COOK, Ian R. *Platforms, sex work and their interconnectedness.* **Sexualities**, v. 26, n. 3, p. 277-297, 2023. Disponível em: https://journals.sagepub.com/doi/full/10.1177/13634607211023013 Acessado em: 21/06/2023.

THOMPSON, John B. Ideologia e Cultura Moderna: teoria social crítica na era da comunicação de massa. **Petrópolis, RJ: Editora Vozes,** 2011.

TOMMASI, Sara *et al.* Approvato il “Digital Services Act”: Regolamento (UE) 2022/2065 del 19.10. 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE. **PERSONA E MERCATO**, v. 4, p. 698-701, 2022. Disponível em: https://iris.unisalento.it/bitstream/11587/495066/1/Approvato%20il%20%E2%80%98Digital%20Services%20Act%E2%80%99%2C%20Persona%20e%20Mercato%202022.pdf Acessado em:11/11/2023.

TWITTER. Privacy Policy 1. 14 mai. 2007. Disponível em: https://Twitter.com/pt/privacy/previous/version_1 Acessado em: 01/06/2022.

_____. Termos de Serviço 1. 2009a. Disponível em: https://Twitter.com/pt/tos/previous/version_1 Acessado em: 01/06/2022.

_____. Termos de Serviço 2. 10 set. 2009b. https://Twitter.com/pt/tos/previous/version_2 Acessado em: 01/06/2022.

_____. Termos de Serviço 3. 18 set. 2009c. https://Twitter.com/pt/tos/previous/version_3 Acessado em: 01/06/2022.

_____. Privacy Policy 2. 18 nov. 2009d. Disponível em: https://Twitter.com/pt/privacy/previous/version_2 Acessado em: 01/06/2022.

_____. Privacy Policy 3. 8 jun. 2010a. Disponível em: https://Twitter.com/pt/privacy/previous/version_3 Acessado em: 01/06/2022.

_____. Privacy Policy 4. 16 nov. 2010b. Disponível em: 0https://Twitter.com/pt/privacy/previous/version_4 Acessado em: 01/06/2022.

_____. Termos de Serviço 4. 16 nov. 2010c. Disponível em: https://Twitter.com/pt/tos/previous/version_4 Acessado em: 01/06/2022.

_____. Termos de Serviço 5. 1 jun. 2011a. Disponível em: https://Twitter.com/pt/tos/previous/version_5 Acessado em: 01/06/2022.

_____. Privacy Policy 5. 23 jun. 2011b. Disponível em: https://Twitter.com/pt/privacy/previous/version_5 Acessado em: 01/06/2022.

_____. Política de Privacidade 6. 17 mai. 2012a. Disponível em: https://Twitter.com/pt/privacy/previous/version_6 Acessado em: 01/06/2022.

_____. Termos de Serviço 6. 17 mai. 2012b. Disponível em: https://Twitter.com/pt/tos/previous/version_6 Acessado em: 01/06/2022.

_____. Termos de Serviço 7. 25 jun. 2012c. Disponível em: https://Twitter.com/pt/tos/previous/version_7 Acessado em: 01/06/2022.

_____. Política de Privacidade 7. 3 jul. 2013a. Disponível em: https://Twitter.com/pt/privacy/previous/version_7 Acessado em: 01/06/2022.

_____. Política de Privacidade 8. 8 out. 2013b. Disponível em: https://Twitter.com/pt/privacy/previous/version_8 Acessado em: 01/06/2022.

_____. Sobre Aplicativos de Terceiros e Sessões de Acesso. 14 de abr. 2014

https://help.Twitter.com/pt/managing-your-account/connect-or-revoke-access-to-third-party-apps Acessado em: 01/06/2022.

_____. Política de Privacidade 9. 8 set. 2014a. Disponível em: https://Twitter.com/pt/privacy/previous/version_9 Acessado em: 01/06/2022.

_____. Termos de Serviço 8. 8 set. 2014b. Disponível em: https://Twitter.com/pt/tos/previous/version_8 Acessado em: 01/06/2022.

_____. Developer Policy. 8 de out. 2014c. Disponível: https://developer.Twitter.com/en/developer-terms/policy Acessado em: 01/06/2022.

_____. Política de Privacidade 10. 17 abr. 2015a. Disponível em: https://Twitter.com/pt/privacy/previous/version_10 Acessado em: 01/06/2022.

_____. Termos de Serviço 9. 18 mai. 2015b. Disponível em: https://Twitter.com/pt/tos/previous/version_9 Acessado em: 01/06/2022.

_____. Política de Privacidade 11. 27 jan. 2016a. Disponível em: https://Twitter.com/pt/privacy/previous/version_11 Acessado em: 01/06/2022.

_____. Termos de Serviço 10. 27 jan. 2016b. Disponível em: https://Twitter.com/pt/tos/previous/version_10 Acessado em: 01/06/2022.

_____. Política de Privacidade 12. 30 set. 2016c. Disponível em: https://Twitter.com/pt/privacy/previous/version_12 Acessado em: 01/06/2022.

_____. Termos de Serviço 11. 30 set. 2016d. Disponível em: https://Twitter.com/pt/tos/previous/version_11 Acessado em: 01/06/2022.

_____. Política de Privacidade 13. 18 jun. 2017a. Disponível em: https://Twitter.com/pt/privacy/previous/version_13 Acessado em: 01/06/2022.

_____. Termos de Serviço 12. 02 out. 2017b. Disponível em: https://Twitter.com/pt/tos/previous/version_12 Acessado em: 01/06/2022.

_____. Política de Privacidade 14. 25 mai. 2018a. Disponível em: https://Twitter.com/pt/privacy/previous/version_14 Acessado em: 01/06/2022.

_____. Termos de Serviço 13. 25 mai. 2018b. Disponível em: https://Twitter.com/pt/tos/previous/version_13 Acessado em: 01/06/2022.

_____. Política contra ameaças violentas, mar. 2019a. Disponível em: https://help.Twitter.com/pt/rules-and-policies/violent-threats-glorification Acessado em: 01/08/2022

_____. Política contra glorificação da violência, mar. 2019b. Disponível em: https://help.Twitter.com/pt/rules-and-policies/glorification-of-violence Acessado em: 01/08/2022

_____. Política de marcas registradas, mar. 2019c. Disponível em: https://help.Twitter.com/pt/rules-and-policies/Twitter-trademark-policy Acessado em: 01/08/2022

_____. Produtos ou serviços ilegais ou regulamentados, abr. 2019d. Disponível em:

https://help.Twitter.com/pt/rules-and-policies/regulated-goods-services Acessado em: 01/08/2022

_____. Política relacionada a nudez não consensual, nov. 2019d. Disponível em: https://help.Twitter.com/pt/rules-and-policies/intimate-media Acessado em: 01/08/2022
TWITTER. About Twitter. 2020a. Disponível em: https://about.Twitter.com/content/dam/about-Twitter/en/company/global-impact-2020.pdf acessado em 05/11/2021.

_____. Política de Privacidade 15. 1 jan. 2020b. Disponível em: https://Twitter.com/pt/privacy/previous/version_15 Acessado em: 01/06/2022.

_____. Termos de Serviço 14. 1 jan. 2020c. Disponível em: https://Twitter.com/pt/tos/previous/version_14 Acessado em: 01/06/2022.

_____. Política de Privacidade 16. 18 jun. 2020d. Disponível em: https://Twitter.com/pt/privacy/previous/version_16 Acessado em: 01/06/2022.

_____. Termos de Serviço 15. 18 jun. 2020e. Disponível em: https://Twitter.com/pt/tos/previous/version_15 Acessado em: 01/06/2022.

_____. Nossa abordagem de bloqueio de link. jul. 2020f. Disponível em: https://help.Twitter.com/pt/safety-and-security/phishing-spam-and-malware-links Acessado em: 01/06/2022.

_____. Política contra organizações violentas, out. 2020g. Disponível em: https://help.Twitter.com/pt/rules-and-policies/violent-groups Acessado em: 01/08/2022

_____. Política contra exploração sexual de menores, out. 2020h. Disponível em: https://help.Twitter.com/pt/rules-and-policies/sexual-exploitation-policy Acessado em: 01/08/2022

_____. Política de Privacidade 17. 19 ago. 2021a. Disponível em: https://Twitter.com/pt/privacy/previous/version_17 Acessado em: 01/06/2022.

_____. Termos de Serviço 16. 19 ago. 2021b. Disponível em: https://Twitter.com/pt/tos/previous/version_16 Acessado em: 01/06/2022.

_____. Política de integridade cívida, out. 2021c. Disponível em: https://about.Twitter.com/content/dam/about-Twitter/en/company/global-impact-2020.pdf Acessado em 05/11/2021.

_____. Política contra autores de ataques violentos, abr. 2022a. Disponível em: https://help.Twitter.com/pt/rules-and-policies/perpetrators-of-violent-attacks Acessado em: 22/06/2022.

_____. Política contra spam e manipulação de plataforma, abr. 2022b. Disponível em: https://help.Twitter.com/pt/rules-and-policies/platform-manipulation Acessado em: 22/06/2022.

_____. Política informações privadas e mídia, abr. 2022c. Disponível em: https://help.Twitter.com/pt/rules-and-policies/platform-manipulation Acessado em: 22/06/2022.

_____. Política de Privacidade 18. 10 jun. 2022d. Disponível em:

https://Twitter.com/pt/privacy Acessado em: 22/06/2022.

_____. Termos de Serviço 17. 10 jun. 2022e. Disponível em: https://Twitter.com/pt/tos Acessado em: 22/06/2022.

_____. As regras do Twitter, 10 jun. 2022f. Disponível em: https://help.Twitter.com/pt/rules-and-policies/Twitter-rules Acessado em: 01/08/2022

_____. Comportamento abusivo, 10 jun. 2022g. Disponível em: https://help.Twitter.com/pt/rules-and-policies/abusive-behavior Acessado em: 01/08/2022

_____. Política contra propagação de ódio, 10 jun. 2022h. Disponível em: https://help.Twitter.com/pt/rules-and-policies/hateful-conduct-policy Acessado em: 01/08/2022

_____. Sobre o assédio online, 10 jun. 2022i. Disponível em: https://help.Twitter.com/pt/safety-and-security/cyber-bullying-and-online-abuse Acessado em: 01/08/2022

_____. Denunciar um comportamento abusivo, 10 jun. 2022j. Disponível em: https://help.Twitter.com/pt/safety-and-security/report-abusive-behavior Acessado em: 01/08/2022

_____. Como ajudar um usuário de assédio online, 10 jun. 2022k. Disponível em: https://help.Twitter.com/pt/safety-and-security/helping-with-online-abuse Acessado em: 01/08/2022

_____. Sobre conteúdo ofensivo, 10 jun. 2022l. Disponível em: https://help.Twitter.com/pt/safety-and-security/offensive-tweets-and-content Acessado em: 01/08/2022

_____. Política de automutilação e suicídio, 10 jun. 2022m. Disponível em: https://help.Twitter.com/pt/rules-and-policies/glorifying-self-harm Acessado em: 01/08/2022

_____. O que fazer em caso de preocupação com automutilação e suicídio no Twitter, 10 jun. 2022n. Disponível em: https://help.Twitter.com/pt/safety-and-security/self-harm-and-suicide Acessado em: 01/08/2022

_____. Denúncia mídia sensível, 10 jun. 2022o. Disponível em: https://help.Twitter.com/pt/safety-and-security/sensitive-media Acessado em: 01/08/2022

_____. Sobre aplicativos para “seguidores gratuitos”, 10 jun. 2022p. Disponível em: https://help.Twitter.com/pt/safety-and-security/free-Twitter-followers-policy Acessado em: 01/08/2022

_____. Sobre links inseguros, 10 jun. 2022q. Disponível em: https://help.Twitter.com/pt/safety-and-security/about-unsafe-links Acessado em: 01/08/2022

_____. Sobre a segurança da conta, 10 jun. 2022r. Disponível em: https://help.Twitter.com/pt/safety-and-security/account-security-tips Acessado em: 01/08/2022

_____. Política de direitos autorais, 10 jun. 2022s. Disponível em: https://help.Twitter.com/pt/rules-and-policies/copyright-policy Acessado em: 01/08/2022

_____. Política sobre mídia sintética e manipulada, 10 jun. 2022t. Disponível em: https://help.Twitter.com/pt/rules-and-policies/manipulated-media Acessado em: 01/08/2022

_____. Como controlar a sua experiência no Twitter, 10 jun. 2022u. Disponível em: https://help.Twitter.com/pt/safety-and-security/control-your-Twitter-experience Acessado em: 01/08/2022

_____. Sobre as configurações de visibilidade do perfil, 10 jun. 2022v. Disponível em: https://help.Twitter.com/pt/safety-and-security/birthday-visibility-settings Acessado em: 01/08/2022

_____. Sobre tweets públicos e protegidos, 10 jun. 2022x. Disponível em: https://help.Twitter.com/pt/safety-and-security/public-and-protected-tweets Acessado em: 01/08/2022

_____. Como proteger e desproteger seus tweets, 10 jun. 2022w. Disponível em: https://help.Twitter.com/pt/safety-and-security/how-to-make-Twitter-private-and-public Acessado em: 01/08/2022

_____. Política de identidades enganosas e que induzem a erro, 10 jun. 2022y. Disponível em: https://help.Twitter.com/pt/rules-and-policies/Twitter-impersonation-and-deceptive-identities-policy Acessado em: 01/08/2022

_____. Política de contas paródias, comentários e fãs-clubes 10 jun. 2022z. Disponível em: https://help.Twitter.com/pt/rules-and-policies/parody-account-policy Acessado em: 01/08/2022

_____. Sobre o rastreamento de idade no Twitter, 10 jun. 2022a2. Disponível em: https://help.Twitter.com/pt/safety-and-security/age-verification Acessado em: 01/08/2022

_____. Ajuda para a minha conta comprometida, 10 jun. 2022b2. Disponível em: https://help.Twitter.com/pt/safety-and-security/Twitter-account-compromised Acessado em: 01/08/2022

_____. Normas de monetização de conteúdo, 10 jun. 2022c2. Disponível em: https://help.Twitter.com/pt/rules-and-policies/content-monetization-standards Acessado em: 01/08/2022

_____. Amplify pre-roll Publisher program FAQs, 10 jun. 2022d2. Disponível em: https://business.Twitter.com/en/help/troubleshooting/amplify-publisher-faqs.html Acessado em: 01/08/2022

_____. Política do Super Follow, 10 jun. 2022e2. Disponível em: https://help.Twitter.com/pt/rules-and-policies/super-follows-policy Acessado em: 01/08/2022

_____. Sobre criadores do Super Follow, 10 jun. 2022f2. Disponível em: https://help.Twitter.com/pt/using-Twitter/super-follows-creator Acessado em: 01/08/2022

_____. Política de espaços com ingressos, 10 jun. 2022g2. Disponível em: https://help.Twitter.com/pt/rules-and-policies/ticketed-spaces-policy Acessado em: 01/08/2022

UNITED STATE. Public Law Nº 110-385, 10 de outubro, 2008. *Broadband Data Improvement Act. To improve the quality of Federal and State data regarding the availability*

and quality of broadband services and to promote the deployment of affordable broadband services to all parts of the Nation. Disponível em: https://www.govinfo.gov/content/pkg/PLAW-110publ385/html/PLAW-110publ385.htm Acessado em: 01/09/2023.

____. Public Law Nº 110-401, 13 de outubro, 2008. *'Providing Resources, Officers, and Technology To Eradicate Cyber Threats to Our Children Act. To require the Department of Justice to develop and implement a National Strategy Child Exploitation Prevention and Interdiction, to improve the Internet Crimes Against Children Task Force, to increase resources for regional computer forensic labs, and to make other improvements to increase the ability of law enforcement agencies to investigate and prosecute child predators.* Disponível em: https://www.govinfo.gov/content/pkg/PLAW-110publ401/pdf/PLAW-110publ401.pdf Acessado em: 01/09/2023.

____. Federal Trade Comission Rule Amendment Vol. 78 Nº 12, 17 de janeiro, 2013. *Children's Online Privacy Protection Rule: The Commission amends the Children's Online Privacy Protection Rule ("COPPA Rule" or "Rule"), consistent with the requirements of the Children's Online Privacy Protection Act, to clarify the scope of the Rule and strengthen its protections for children's personal information, in light of changes in online technology since the Rule went into effect in April 2000.* Disponível em: https://www.ftc.gov/system/files/2012-31341.pdf Acessado em: 01/09/2023.

____. Public Law Nº 115-164, 11 de abril, 2018. *Allow States and Victims to Fight Online Sex Trafficking Act: To amend the Communications Act of 1934 to clarify that section 230 of such Act does not prohibit the enforcement against providers and users of interactive computer services of Federal and State criminal and civil law relating to sexual exploitation of children or sex trafficking, and for other purposes.* Disponível em: https://www.congress.gov/115/plaws/publ164/PLAW-115publ164.pdf Acessado em: 01/09/2023.

____. Senate and House of Representative. *Internet Freedom Preservation Act.* **Projeto de Lei nº 215/5353, de 9 de janeiro de 2007**. *To amend the Communications Act of 1934 to ensure net neutrality*. Washington: Congress, 2007. Disponível em: https://www.govinfo.gov/content/pkg/BILLS-110s215is/pdf/BILLS-110s215is.pdf Acessado em: 01/09/2023.

____. Senate. *Counter Spy Act.* **Projeto de Lei nº 1625, de 14 de junho de 2007**. *To protect against the unauthorized installation of computer software, to require clear disclosure to computer users of certain computer software features that may pose a threat to user privacy, and for other purposes.* Washington: Congress, 2007. Disponível em: https://www.govinfo.gov/content/pkg/BILLS-110s1625is/pdf/BILLS-110s1625is.pdf Acessado em: 01/09/2023.

____. House of Representative. *Responsible and Effective Solutions for Children Using and Entering Online Services Act.* **Projeto de Lei nº 3850, de 16 de outubro de 2007**. *To improve the collection and use of data related to crimes of child exploitation, and for other purposes*. Washington: Congress, 2007. Disponível em: https://www.govinfo.gov/content/pkg/BILLS-110hr3850ih/pdf/BILLS-110hr3850ih.pdf Acessado em: 01/09/2023.

____. House of Representative. *E-fencing Enforcement Act.* **Projeto de Lei nº 6713/1166, de 31 de julho de 2008**. *To amend title 18, United States Code, to provide for more effective enforcement of the Federal prohibition on the interstate shipment of stolen property, and for other purposes*. Washington: Congress, 2008. Disponível em:

https://www.congress.gov/110/bills/hr6713/BILLS-110hr6713ih.pdf Acessado em: 01/09/2023.

____. House of Representative. *Online Age Verification and Child Safety Act.* **Projeto de Lei nº 4059, de 06 de novembro de 2009**. *To enhance Internet safety and security and to prevent exploitation of children online through the use of technology.* Washington: Congress, 2009. Disponível em: https://www.congress.gov/111/bills/hr4059/BILLS-111hr4059ih.pdf Acessado em: 01/09/2023.

____. Senate. *Combating Online Infringement and Counterfeits Act.* **Projeto de Lei nº 3804, de 20 de setembro de 2010**. *To combat online infringement, and for other purposes.* Washington: Congress, 2010. Disponível em: https://www.congress.gov/111/bills/s3804/BILLS-111s3804rs.pdf Acessado em: 01/09/2023.

____. Senate. *Do-Not-Track Online Act.* **Projeto de Lei nº 913/418/2404, de 09 de maio de 2011**. *To require the Federal Trade Commission to prescribe regulations regarding the collection and use of personal information obtained by tracking the online activity of an individual, and for other purposes.* Washington: Congress, 2011. Disponível em: https://www.congress.gov/112/bills/s913/BILLS-112s913is.pdf Acessado em: 01/09/2023.

____. Senate. *Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property - PROTECT IP Act.* **Projeto de Lei nº 968, de 12 de maio de 2011** *To prevent online threats to economic creativity and theft of intellectual property, and for other purposes.* Washington: Congress, 2011. Disponível em: https://www.congress.gov/112/bills/s968/BILLS-112s968rs.pdf Acessado em: 01/09/2023

____. House of Representative and Senate. *Do-Not-Track Kids Act.* **Projeto de Lei nº 1895/1700/3481/1563/2734/2932/5930, de 13 de maio de 2011** *To amend the Children's Online Privacy Protection Act of 1998 to extend, enhance, and revise the provisions relating to collection, use, and disclosure of personal information of children and to establish certain other protections for personal information of children and minors.* Washington: Congress, 2011. Disponível em: https://www.congress.gov/112/bills/hr1895/BILLS-112hr1895ih.pdf Acessado em: 01/09/2023

____. House of Representative. *Stop Online Piracy Act.* **Projeto de Lei nº 3261, de 26 de outubro de 2011** *To promote prosperity, creativity, entrepreneurship, and innovation by combating the theft of U.S. property, and for other purposes.* Washington: Congress, 2011. Disponível em: https://www.congress.gov/112/bills/hr3261/BILLS-112hr3261ih.pdf Acessado em: 01/09/2023

____. Senate and House of Representative. - *Online Protection and Enforcement of Digital Trade Act – OPEN Act.* **Projeto de Lei nº 2029/3782, de 17 de dezembro de 2011** *To amend the Tariff Act of 1930 to deter unfair imports that infringe United States intellectual property rights, and for other purposes.* Washington: Congress, 2011. Disponível em: https://www.congress.gov/112/bills/s2029/BILLS-112s2029is.pdf Acessado em: 01/09/2023

____. House of Representative. *Mobile Device Privacy Act.* **Projeto de Lei nº 6377, de 12 de setembro de 2012** *To require disclosures to consumers regarding the capability of software to monitor mobile device usage, to require the express consent of the consumer prior to monitoring, and for other purposes.* Washington: Congress, 2012. Disponível em: https://www.congress.gov/112/bills/hr6377/BILLS-112hr6377ih.pdf Acessado em: 01/09/2023

____. House of Representative. *Global Online Freedom Act.* **Projeto de Lei nº 491, de 04 de fevereiro de 2013** *To prevent United States businesses from cooperating with repressive governments in transforming the Internet into a tool of censorship and surveillance, to fulfill*

the responsibility of the United States Government to promote freedom of expression on the Internet, to restore public confidence in the integrity of United States businesses, and for other purposes. Washington: Congress, 2013. Disponível em: https://www.congress.gov/113/bills/hr491/BILLS-113hr491ih.pdf Acessado em: 01/09/2023

____. House of Representative. *Online Communications and Geolocation Protection Act.* **Projeto de Lei nº 983/656, de 06 de março de 2013** *To amend title 18, United States Code, with respect to disclosures to governments by communications-related service providers of certain information consisting of or relating to communications, and for other purposes.* Washington: Congress, 2013. Disponível em: https://www.congress.gov/113/bills/hr983/BILLS-113hr983ih.pdf Acessado em: 01/09/2023

____. House of Representative and Senate. *Geolocational Privacy and Surveillance Act.* **Projeto de Lei nº 1312/639, de 21 de março de 2013** *To amend title 18, United States Code, to specify the circumstances in which a person may acquire geolocation information and for other purposes.* Washington: Congress, 2013. Disponível em: https://www.congress.gov/113/bills/s639/BILLS-113s639is.pdf Acessado em: 01/09/2023

____. House of Representative. *Forbidding Advertisement Through Child Exploitation - FACE Act.* **Projeto de Lei nº 2645, de 10 de julho de 2013** *To prohibit providers of social media services from using self-images uploaded by minors for commercial purposes.* Washington: Congress, 2013. Disponível em: https://www.govinfo.gov/content/pkg/BILLS-113hr2645ih/pdf/BILLS-113hr2645ih.pdf Acessado em: 01/09/2023

____. House of Representative and Senate. *Geolocational Commercial Privacy Bill of Rights Act.* **Projeto de Lei nº 4711/2378/1053/547/4543/2187, de 21 de maio de 2014** *To establish a regulatory framework for the comprehensive protection of personal data for individuals under the aegis of the Federal Trade Commission, to amend the Children's Online Privacy Protection Act of 1998 to improve provisions relating to collection, use, and disclosure of personal information of children, and for other purposes.* Washington: Congress, 2014. Disponível em: https://www.congress.gov/113/bills/hr4711/BILLS-113hr4711ih.pdf Acessado em: 01/09/2023

____. Senate and House of Representative. *Law Enforcement Access to Data Stored Abroad Act.* **Projeto de Lei nº 2871/512/1174, de 21 de maio de 2014** *To amend title 18, United States Code, to safeguard data stored abroad from improper government access, and for other purposes.* Washington: Congress, 2014. Disponível em: https://www.congress.gov/113/bills/s2871/BILLS-113s2871is.pdf Acessado em: 01/09/2023

____. House of Representative. *Customer Non-Discrimination Act.* **Projeto de Lei nº 5586/3520/2687/5744, de 18 de junho de 2016** *To prohibit discrimination in public accommodations on the basis of sex, gender identity, and sexual orientation, and for other purposes.* Congress, 2016. Disponível em: https://www.govinfo.gov/content/pkg/BILLS-113hr2645ih/pdf/BILLS-113hr2645ih.pdf Acessado em: 01/09/2023

____. House of Representative. *Online Privacy Act.* **Projeto de Lei nº 3175/4978/6027, de 18 de julho de 2017** *To establish privacy protections for customers of broadband Internet access service and other telecommunications services.* Congress, 2017. Disponível em: https://www.govinfo.gov/content/pkg/BILLS-113hr2645ih/pdf/BILLS-113hr2645ih.pdf Acessado em: 01/09/2023

____. Senate. *Social Media Privacy Protection and Consumer Rights.* **Projeto de Lei nº 2728/189/1667, de 23 de abril de 2018** *To protect the privacy of users of social media and other online platforms.* Washington: Congress, 2018. Disponível em: https://www.congress.gov/115/bills/s2728/BILLS-115s2728is.pdf Acessado em: 01/09/2023

____. Senate. *Customer Online Notification for Stopping Edge-provider Network Transgressions - CONSENT Act.* **Projeto de Lei nº 2639/5815, de 10 de abril de 2018** *To protect the right of the American public under the First Amendment to the Constitution of the United States to receive news and information from disparate sources by regulating the use of automated software programs intended to impersonate or replicate human activity on social media.* Washington: Congress, 2018. Disponível em: https://www.congress.gov/115/bills/s3127/BILLS-115s3127is.pdf Acessado em: 01/09/2023

____. Senate and House of Representative. *Bot Disclosure and Accountability Act.* **Projeto de Lei nº 3127/2125/4536, de 25 de junho de 2018** *To require the Federal Trade Commission to establish privacy protections for customers of online edge providers, and for other purposes.* Washington: Congress, 2018. Disponível em: https://www.govinfo.gov/content/pkg/BILLS-115s2639is/pdf/BILLS-115s2639is.pdf Acessado em: 01/09/2023

____. House of Representative. *Remove Explicit Material Offensive to Victims Expeditiously Act - REMOVE Act.* **Projeto de Lei nº 6917/8013, de 26 de setembro de 2018** *To protect victims of nonconsensual online distribution of sexually intimate images by providing for the expeditious removal of nonconsensual sexually intimate imagery on the Internet, to encourage responsible practices by online service providers, and for other purposes.* Congress, 2018. Disponível em: https://www.congress.gov/115/bills/s3744/BILLS-115s3744is.pdf Acessado em: 01/09/2023

____. Senate. *Data CARE Act.* **Projeto de Lei nº 3744/2961/919, de 12 de dezembro de 2018** *To establish duties for online service providers with respect to end user data that such providers collect and use.* Washington: Congress, 2018. Disponível em: https://www.govinfo.gov/content/pkg/BILLS-115s2639is/pdf/BILLS-115s2639is.pdf Acessado em: 01/09/2023

____. House of Representative. *Biased Algorithm Deterrence Act.* **Projeto de Lei nº 7363/492, de 20 de dezembro de 2018** *To amend the Communications Act of 1934 to provide that an owner or operator of a social media service that hinders the display of user-generated content shall be treated as a publisher or speaker of such content, and for other purposes.* Congress, 2018. Disponível em: https://www.govinfo.gov/content/pkg/BILLS-115hr7363ih/pdf/BILLS-115hr7363ih.pdf Acessado em: 01/09/2023

____. Senate. *Own Your Own Data Act.* **Projeto de Lei nº 806, de 14 de março de 2019** *To prohibit the collection of data or information generated on the internet.* Washington: Congress, 2019. Disponível em: https://www.govinfo.gov/content/pkg/BILLS-115s2639is/pdf/BILLS-115s2639is.pdf Acessado em: 01/09/2023

____. Senate and House of Representative. *Designing Accounting Safeguards to Help Broaden Oversight and Regulations on Data – DASHBOARD Act.* **Projeto de Lei nº 1951/8512/7120, de 25 de junho de 2019** *To require the Securities and Exchange Commission to promulgate regulations relating to the disclosure of certain commercial data, and for other purposes.* Washington: Congress, 2019. Disponível em: https://www.congress.gov/116/bills/s1951/BILLS-116s1951is.pdf Acessado em: 01/09/2023

____. Senate. *Ending Support for Internet Censorship Act.* **Projeto de Lei nº 1914, de 19 de junho de 2019** *To amend the Communications Decency Act to encourage providers of interactive computer services to provide content moderation that is politically neutral.* Washington: Congress, 2019. Disponível em: https://www.congress.gov/116/bills/s1914/BILLS-116s1914is.pdf Acessado em: 01/09/2023

____. House of Representative. *Stop the Censorship Act.* **Projeto de Lei nº 4027/7808/8612, de 25 de julho de 2019** *To amend section 230 of the Communications Act of 1934 (commonly referred to as the Communications Decency Act) to stop censorship, and for other purposes.* Washington: Congress, 2019. Disponível em: https://www.congress.gov/116/bills/hr4027/BILLS-116hr4027ih.pdf Acessado em: 01/09/2023

____. Senate. *Social Media Addiction Reduction Technology Act - SMART Act.* **Projeto de Lei nº 2314, de 30 de julho de 2019** *To To prohibit social media companies from using practices that exploit human psychology or brain physiology to substantially impede freedom of choice, to require social media companies to take measures to mitigate the risks of internet addiction and psychological exploitation, and for other purposes.* Washington: Congress, 2019. Disponível em: https://www.congress.gov/116/bills/s2314/BILLS-116s2314is.pdf Acessado em: 01/09/2023

____. House of Representative. *Protecting Local Authority and Neighborhoods Act - PLAN Act.* **Projeto de Lei nº 4232/1107, de 06 de setembro de 2019.** *To amend the Communications Act of 1934 to ensure the ability to enforce State and local law relating to leasing and renting of real property, and for other purposes.* Washington: Congress, 2019. Disponível em: https://www.congress.gov/116/bills/hr4027/BILLS-116hr4027ih.pdf Acessado em: 01/09/2023

____. House of Representative. *National Commission on Online Platforms and Homeland Security Act.* **Projeto de Lei nº 4782, de 22 de outubro de 2019.** *To establish a national commission on online platforms and homeland security, and for other purposes.* Washington: Congress, 2019. Disponível em: https://www.congress.gov/116/bills/hr4782/BILLS-116hr4782rh.pdf Acessado em: 01/09/2023

____. House of Representative. *Keep Big Tech Out of Finance Act.* **Projeto de Lei nº 4813, de 23 de outubro de 2019.** *To prohibit large platform utilities from being a financial institution or being affiliated with a person that is a financial institution, and for other purposes.* Washington: Congress, 2019. Disponível em: https://www.congress.gov/116/bills/hr4813/BILLS-116hr4813ih.pdf Acessado em: 01/09/2023

____. House of Representative. *Raising the Bar Act.* **Projeto de Lei nº 5209, de 21 de novembro de 2019.** *To direct the Under Secretary for Science and Technology of the Department of Homeland Security to design and administer a voluntary online terrorist content moderation exercise program, and for other purposes.* Washington: Congress, 2019. Disponível em: https://www.congress.gov/116/bills/hr5209/BILLS-116hr5209ih.pdf Acessado em: 01/09/2023

____. House of Representative. *Eliminate Network Distribution of Child Exploitation Act - END Child Exploitation Act.* **Projeto de Lei nº 5376/3007/1198/365, de 10 de dezembro de 2019.** *To amend title 18, United States Code, to require a provider of a report to the CyberTipline related to online sexual exploitation of children to preserve the contents of such report for 180 days, and for other purposes.* Washington: Congress, 2019. Disponível em: https://www.congress.gov/116/bills/hr5376/BILLS-116hr5376ih.pdf Acessado em: 01/09/2023

____. House of Representative. *Combating Online Wildlife Trafficking Act.* **Projeto de Lei nº 5398/1546, de 11 de dezembro de 2019.** *To amend the Eliminate, Neutralize, and Disrupt Wildlife Trafficking Act of 2016 to direct the Presidential Task Force on Wildlife Trafficking to develop recommendations to address wildlife trafficking on the internet and on social media, and to direct the Secretary of State and the Administrator of the United States Agency for International Development to develop a strategy to address wildlife trafficking on the internet*

and on social media, and for other purposes. Washington: Congress, 2019. Disponível em: https://www.congress.gov/116/bills/hr5398/BILLS-116hr5398ih.pdf Acessado em: 01/09/2023

____. Senate and House of Representative. *Eliminating Abusive and Rampant Neglect of Interactive Technologies Act - EARN IT Act.* **Projeto de Lei nº 3398/8454/3538/6544, de 05 de março de 2020.** *To establish a National Commission on Online Child Sexual Exploitation Prevention, and for other purposes.* Washington: Congress, 2020. Disponível em: https://www.congress.gov/116/bills/s3398/BILLS-116s3398rs.pdf Acessado em: 01/09/2023

____. Senate and House of Representative. *TikTok on Government Devices Act.* **Projeto de Lei nº 3455/6896/1143/2566, de 12 de março de 2020.** *To prohibit certain individuals from downloading or using TikTok on any device issued by the United States or a government corporation.* Washington: Congress, 2020. Disponível em: https://www.congress.gov/116/bills/s3455/BILLS-116s3455es.pdf Acessado em: 01/09/2023

____. House of Representative. *Social Media Accountability and Account Verification Act.* **Projeto de Lei nº 6586/4653, de 21 de abril de 2020.** *To prohibit the creation and use of fake social media accounts or profiles and the sending of fraudulent emails or other electronic messages, and to require certain social media companies to remove fake or harmful accounts and profiles from their platforms.* Washington: Congress, 2020. Disponível em: https://www.govinfo.gov/content/pkg/BILLS-116hr6586ih/pdf/BILLS-116hr6586ih.pdf Acessado em: 01/09/2023

____. House of Representative. *Social Media Fraud Mitigation Act.* **Projeto de Lei nº 6587/4654, de 21 de abril de 2020.** *To prohibit the creation and use of fake social media accounts or profiles and the sending of fraudulent emails or other electronic messages.* Washington: Congress, 2020. Disponível em: https://www.congress.gov/116/bills/hr6587/BILLS-116hr6587ih.pdf Acessado em: 01/09/2023

____. Senate and House of Representative. *Invest in Child Safety Act.* **Projeto de Lei nº 3629/6752/807/223, de 06 de maio de 2020.** *To establish the Office to Enforce and Protect Against Child Sexual Exploitation.* Washington: Congress, 2020. Disponível em: https://www.congress.gov/116/bills/s3629/BILLS-116s3629is.pdf Acessado em: 01/09/2023

____. Senate and House of Representative. *Limiting Section 230 Immunity to Good Samaritans Act.* **Projeto de Lei nº 3983/8596, de 17 de junho de 2020.** *To amend the Communications Act of 1934 to provide accountability for bad actors who abuse the Good Samaritan protections provided under that Act, and for other purposes.* Washington: Congress, 2020. Disponível em https://www.congress.gov/116/bills/s3983/BILLS-116s3983is.pdf Acessado em: 01/09/2023

____. Senate. *Stopping Big Tech's Censorship Act.* **Projeto de Lei nº 4062, de 22 de junho de 2020.** *To amend section 230 of the Communications Act of 1934 to require that providers and users of an interactive computer service meet certain standards to qualify for liability protections.* Washington: Congress, 2020. Disponível em https://www.govinfo.gov/content/pkg/BILLS-116s4062is/pdf/BILLS-116s4062is.pdf Acessado em: 01/09/2023

____. House of Representative. *Defund Executive Orders that Suppress Free Speech Act.* **Projeto de Lei nº 7300, de 22 de junho de 2020.** *To prevent Federal funds from being used to carry out Executive Order 13925, and for other purposes.* Washington: Congress, 2020. Disponível em: https://www.congress.gov/116/bills/hr7300/BILLS-116hr7300ih.pdf Acessado em: 01/09/2023

____. Senate. *Platform Accountability and Consumer Transparency Act - PACT Act.* **Projeto de Lei nº 4066/797, de 24 de junho de 2020.** *To require transparency, accountability, and protections for consumers online.* Washington: Congress, 2020. Disponível em https://www.congress.gov/116/bills/s4066/BILLS-116s4066is.pdf Acessado em: 01/09/2023

____. Senate. *Online Freedom and Viewpoint Diversity Act.* **Projeto de Lei nº 4534, de 08 de setembro de 2020.** *To amend section 230 of the Communications Act of 1934 to modify the scope of protection from civil liability for "good Samaritan" blocking and screening of offensive material.* Washington: Congress, 2020. Disponível em https://www.congress.gov/116/bills/s4534/BILLS-116s4534is.pdf Acessado em: 01/09/2023

____. Senate. *Online Content Policy Modernization Act.* **Projeto de Lei nº 4632, de 21 de setembro de 2020.** *To amend title 17, United States Code, to establish an alternative dispute resolution program for copyright small claims, to amend the Communications Act of 1934 to modify the scope of protection from civil liability for "good Samaritan" blocking and screening of offensive material, and for other purposes.* Washington: Congress, 2020. Disponível em https://www.congress.gov/116/bills/s4632/BILLS-116s4632is.pdf Acessado em: 01/09/2023

____. House of Representative. *Bianca's Law.* **Projeto de Lei nº 8323, de 21 de setembro de 2020.** *To require social media companies to establish an office dedicated to identifying and removing violent and gory content that violates such company's social media platform content moderation standards.* Washington: Congress, 2020. Disponível em https://www.govinfo.gov/content/pkg/BILLS-116hr8323ih/pdf/BILLS-116hr8323ih.pdf Acessado em: 01/09/2023

____. Senate and House of Representative. *Don't Push My Buttons Act.* **Projeto de Lei nº 4756/8515/2335, de 29 de setembro de 2020.** *To amend the Communications Act of 1934 to narrow the scope of the limitation on liability provided under section 230 of that Act, and for other purposes.* Washington: Congress, 2020. Disponível em https://www.govinfo.gov/content/pkg/BILLS-116s4756is/pdf/BILLS-116s4756is.pdf Acessado em: 01/09/2023

____. Senate. *See Something, Say Something Online Act.* **Projeto de Lei nº 4758/27, de 29 de setembro de 2020.** *To require reporting of suspicious transmissions in order to assist in criminal investigations and counterintelligence activities relating to international terrorism, and for other purposes.* Washington: Congress, 2020. Disponível em https://www.congress.gov/116/bills/s4758/BILLS-116s4758is.pdf Acessado em: 01/09/2023

____. House of Representative. *Protect Speech Act.* **Projeto de Lei nº 8517/3827, de 02 de outubro de 2020.** *To amend section 230 of the Communications Act of 1934 to ensure that the immunity under such section incentivizes online platforms to responsibly address illegal content while not immunizing the disparate treatment of ideological viewpoints and continuing to encourage a vibrant, open, and competitive internet, and for other purposes.* Washington: Congress, 2020. Disponível em https://www.congress.gov/116/bills/hr8517/BILLS-116hr8517ih.pdf Acessado em: 01/09/2023

____. House of Representative and Senate. *Protecting Americans from Dangerous Algorithms Act.* **Projeto de Lei nº 8517/3827, de 20 de outubro de 2020.** *To amend section 230(c) of the Communications Act of 1934 to prevent immunity for interactive computer services for certain claims, and for other purposes.* Washington: Congress, 2020. Disponível https://www.congress.gov/116/bills/hr8636/BILLS-116hr8636ih.pdf Acessado em: 01/09/2023

____. Senate. *Stop Suppressing Speech Act.* **Projeto de Lei nº 4828, de 21 de outubro de 2020.** *To amend section 230 of the Communications Act of 1934 (commonly referred to as the "Communications Decency Act") to stop censorship, and for other purposes.*

Washington: Congress, 2020. Disponível em: https://www.congress.gov/116/bills/s4828/BILLS-116s4828is.pdf Acessado em: 01/09/2023

____. House of Representative. *Curbing Abuse and Saving Expression in Technology Act - CASE-IT Act.* **Projeto de Lei nº 8719/285, de 30 de outubro de 2020.** *To amend section 230 of the Communications Act of 1934 to limit the immunity of providers and users of interactive computer services under such section, and for other purposes.* Washington: Congress, 2020. Disponível em: https://www.congress.gov/116/bills/hr8719/BILLS-116hr8719ih.pdf Acessado em: 01/09/2023

____. Senate and House of Representative. *Public Servant Protection Act.* **Projeto de Lei nº 4965/7799, de 03 de dezembro de 2020.** *To regulate the posting of personal information of government officials on the internet, and for other purposes.* Washington: Congress, 2020. Disponível em: https://www.congress.gov/116/bills/s4965/BILLS-116s4965is.pdf Acessado 01/09/2023

____. House of Representative. *Abandoning Online Censorship Act - AOC Act.* **Projeto de Lei nº 8896/874, de 08 de dezembro de 2020.** *To repeal section 230 of the Communications Act of 1934 (commonly referred to as the Communications Decency Act) to stop censorship, and for other purposes.* Washington: Congress, 2020. Disponível em: https://www.congress.gov/116/bills/hr8896/BILLS-116hr8896ih.pdf Acessado 01/09/2023

____. Senate and House of Representative. *Promoting Responsibility Over Moderation in the Social-media Environment - PROMISE Act.* **Projeto de Lei nº 4975/427/5803, de 08 de dezembro de 2020.** *To require covered entities to implement and disclose information moderation policies, and for other purposes.* Washington: Congress, 2020. Disponível em: https://www.govinfo.gov/content/pkg/BILLS-117s427is/pdf/BILLS-117s427is.pdf Acessado 01/09/2023

____. House of Representative. *Break Up Big Tech Act.* **Projeto de Lei nº 8922, de 09 de dezembro de 2020.** *To amend the Communications Act of 1934 to limit interactive computer service immunity.* Washington: Congress, 2020. Disponível em: https://www.congress.gov/116/bills/hr8922/BILLS-116hr8922ih.pdf Acessado 01/09/2023

____. Senate. *Holding Sexual Predators and Online Enablers Accountable Act.* **Projeto de Lei nº 5012, de 11 de dezembro de 2020.** *To amend chapter 110 of title 18, United States Code, to provide for criminal and civil liability for an interactive computer service that willfully or recklessly promotes or facilitates child exploitation, to amend section 230 of the Communications Act of 1934, and for other purposes.* Washington: Congress, 2020. Disponível em: https://www.congress.gov/116/bills/s5012/BILLS-116s5012is.pdf Acessado 01/09/2023

____. Senate. *A bill to repeal section 230 of the Communications Act of 1934.* **Projeto de Lei nº 5020/2972, de 15 de dezembro de 2020.** *To repeal section 230 of the Communications Act of 1934.* Washington: Congress, 2020. Disponível em: https://www.congress.gov/116/bills/hr9043/BILLS-116hr9043ih.pdf Acessado 01/09/2023

____. House of Representative. *Online Terrorism Prevention Act.* **Projeto de Lei nº 9043, de 21 de dezembro de 2020.** *To require social media companies to establish an office dedicated to identifying and removing violent or extremist content associated with or distributed by any entity identified as a terrorist organization.* Washington: Congress, 2020. Disponível em: https://www.congress.gov/116/bills/s5020/BILLS-116s5020is.pdf Acessado 01/09/2023

____. Senate. *A bill to amend the Internal Revenue Code of 1986 to increase the additional 2020 recovery rebates, to repeal section 230 of the Communications Act of 1934, and for other purposes.* **Projeto de Lei nº 5085, de 29 de dezembro de 2020.** *To amend the Internal Revenue Code of 1986 to increase the additional 2020 recovery rebates, to repeal section 230 of the Communications Act of 1934, and for other purposes.* Washington: Congress, 2020. Disponível em: https://www.congress.gov/116/bills/s5085/BILLS-116s5085pcs.pdf Acessado 01/09/2023

____. House of Representative. *Protecting Constitutional Rights from Online Platform Censorship Act.* **Projeto de Lei nº 83, de 04 de janeiro de 2021.** *To amend the Communications Act of 1934 to protect constitutional rights from online platform censorship, and for other purposes.* Washington: Congress, 2021. Disponível em: https://www.congress.gov/117/bills/hr83/BILLS-117hr83ih.pdf Acessado 01/09/2023

____. Senate and House of Representative. *Safeguarding Against Fraud, Exploitation, Threats, Extremism, and Consumer Harms Act - SAFE TECH Act.* **Projeto de Lei nº 299/3421, de 08 de fevereiro de 2021.** *To amend the Communications Act of 1934 to protect constitutional rights from online platform censorship, and for other purposes.* Washington: Congress, 2021. Disponível em: https://www.congress.gov/117/bills/hr83/BILLS-117hr83ih.pdf Acessado 01/09/2023

____. House of Representative. *No Social Media Accounts for Terrorists or State Sponsors of Terrorism Act.* **Projeto de Lei nº 1543, de 03 de março de 2021.** *To provide authorities to prohibit the provision of services by social media platforms to certain individuals and entities on the Specially Designated Nationals List and senior officials of governments of a state sponsor of terrorism.* Washington: Congress, 2021. Disponível em: https://www.congress.gov/117/bills/hr1543/BILLS-117hr1543ih.pdf Acessado 01/09/2023

____. House of Representative. *Stop Shielding Culpable Platforms Act.* **Projeto de Lei nº 2000, de 18 de março de 2021.** *To amend section 230 of the Communications Act of 1934 to clarify that such section does not prevent a provider or user of an interactive computer service from being treated as the distributor of information provided by another information content provider, and for other purposes.* Washington: Congress, 2021. Disponível em: https://www.congress.gov/117/bills/hr2000/BILLS-117hr2000ih.pdf Acessado 01/09/2023

____. Senate and House of Representative. *21st Century Foundation for the Right to Express and Engage in Speech Act - 21st Century FREE Speech Act.* **Projeto de Lei nº 1384/7613, de 27 de abril de 2021.** *To repeal section 230 of the Communications Act of 1934 and ensure reasonable, non-discriminatory access to online communications platforms.* Washington: Congress, 2021. Disponível em: https://www.congress.gov/117/bills/s1384/BILLS-117s1384is.pdf Acessado 01/09/2023

____. House of Representative. *Anti-CCP Espionage via Social Media Act - ACES Act.* **Projeto de Lei nº 3057, de 07 de maio de 2021.** *To require ByteDance to divest itself of certain assets, and to require the Committee on Foreign Investment in the United States to review certain business relationships between ByteDance and United States businesses, and for other purposes.* Washington: Congress, 2021. Disponível em: https://www.congress.gov/117/bills/hr3057/BILLS-117hr3057ih.pdf Acessado 01/09/2023

____. House of Representative. *Civil Rights Modernization Act.* **Projeto de Lei nº 3184, de 13 de maio de 2021.** *To amend section 230 of the Communications Act of 1934 to clarify that such section has no effect on civil rights laws with respect to the targeting of covered advertisements, and for other purposes.* Washington: Congress, 2021. Disponível em: https://www.congress.gov/117/bills/hr3184/BILLS-117hr3184ih.pdf Acessado 01/09/2023

____. House of Representative. *Social Media Disclosure and Transparency of Advertisements Act - Social Media DATA Act.* **Projeto de Lei nº 3451, de 20 de maio de 2021.** *To require covered platforms to provide information about their advertising to academic researchers, and for other purposes.* Washington: Congress, 2021. Disponível em: https://www.congress.gov/117/bills/hr3451/BILLS-117hr3451ih.pdf Acessado 01/09/2023

____. Senate and House of Representative. *Algorithmic Justice and Online Platform Transparency Act.* **Projeto de Lei nº 1896/3611, de 27 de maio de 2021.** *To prohibit the discriminatory use of personal information by online platforms in any algorithmic process, to require transparency in the use of algorithmic processes and content moderation, and for other purposes.* Washington: Congress, 2021. Disponível em: https://www.congress.gov/117/bills/s1896/BILLS-117s1896is.pdf Acessado 01/09/2023

____. Senate. *Promoting Rights and Online Speech Protections to Ensure Every Consumer is Heard Act - PRO-SPEECH Act.* **Projeto de Lei nº 2031, de 16 de junho de 2021.** *To preserve access to lawful content and prevent discrimination and unfair methods of competition on the internet, and for other purposes.* Washington: Congress, 2021. Disponível em: https://www.congress.gov/117/bills/s2031/BILLS-117s2031is.pdf Acessado 01/09/2023

____. Senate. *Disincentivizing Internet Service Censorship of Online Users and Restrictions on Speech and Expression Act - DISCOURSE Act.* **Projeto de Lei nº 2228, de 24 de junho de 2021.** *To amend section 230 of the Communications Act of 1934 to correct shortcomings in how that section addresses content moderation, content creation and development, and content distribution.* Washington: Congress, 2021. Disponível em: https://www.congress.gov/117/bills/s2228/BILLS-117s2228is.pdf Acessado 01/09/2023

____. House of Representative. *User Data Protection Act.* **Projeto de Lei nº 4220, de 29 de junho de 2021.** *To prohibit digital platforms from using information about a user unless the user consents to such use, to ensure personal information is considered a property right, and for other purposes.* Washington: Congress, 2021. Disponível em: https://www.congress.gov/117/bills/hr4240/BILLS-117hr4240ih.pdf Acessado 01/09/2023

____. Senate. *Preserving Political Speech Online Act.* **Projeto de Lei nº 2338, de 14 de julho de 2021.** *To improve fairness in political speech, and for other purposes.* Washington: Congress, 2021. Disponível em: https://www.congress.gov/117/bills/s2338/BILLS-117s2338is.pdf Acessado 01/09/2023

____. Senate. *Health Misinformation Act.* **Projeto de Lei nº 2448, de 22 de julho de 2021.** *To amend the Communications Act of 1934 to provide that, under certain circumstances, an interactive computer service provider that allows for the proliferation of health misinformation through that service shall be treated as the publisher or speaker of that misinformation, and for other purposes.* Washington: Congress, 2021. Disponível em: https://www.congress.gov/117/bills/s2448/BILLS-117s2448is.pdf Acessado 01/09/2023

____. Senate. *PRESERVE Online Speech Act.* **Projeto de Lei nº 2500, de 28 de julho de 2021.** *To require providers of interactive computer services to publicly disclose information relating to requests or recommendations made by government entities to moderate content, and for other purposes.* Washington: Congress, 2021. Disponível em: https://congress.gov/117/bills/s2500/BILLS-117s2500is.pdf Acessado 01/09/2023

____. Senate and House of Representative. *Accountability for Online Firearms Marketplaces Act.* **Projeto de Lei nº 2725/7819, de 13 de setembro de 2021.** *To amend the Communications Decency Act to remove immunity for online firearms marketplaces, and for other purposes.* Washington: Congress, 2021. Disponível em: https://www.congress.gov/117/bills/s2725/BILLS-117s2725is.pdf Acessado 01/09/2023

____. House of Representative and Senate. *Federal Big Tech Tort Act.* **Projeto de Lei nº 5449/2917, de 30 de setembro de 2021.** *To establish a Federal tort against social media companies that cause bodily injury to children or harm the mental health of children.* Washington: Congress, 2021. Disponível em: https://www.congress.gov/117/bills/hr5449/BILLS-117hr5449ih.pdf Acessado 01/09/2023

____. House of Representative. *Justice Against Malicious Algorithms Act.* **Projeto de Lei nº 5596, de 15 de outubro de 2021.** *To amend section 230 of the Communications Act of 1934 to limit the liability protection provided by such section when a provider of an interactive computer service knew or should have known such provider was making a personalized recommendation of third-party information or recklessly made a personalized recommendation of such information, and for other purposes.* Washington: Congress, 2021. Disponível em: https://www.congress.gov/117/bills/hr5596/BILLS-117hr5596ih.pdf Acessado 01/09/2023

____. Senate. *Nudging Users to Drive Good Experiences on Social Media Act - Social Media NUDGE Act.* **Projeto de Lei nº 3608, de 09 de fevereiro de 2022.** *To require the Federal Trade Commission to identify content-agnostic platform interventions to reduce the harm of algorithmic amplification and social media addiction on covered platforms, and for other purposes.* Washington: Congress, 2022. Disponível em: https://www.congress.gov/117/bills/s3608/BILLS-117s3608is.pdf Acessado 01/09/2023

____. House of Representative. *Cooperation Among Police, Tech, and Users to Resist Exploitation Act - CAPTURE Act.* **Projeto de Lei nº 6755, de 12 de fevereiro de 2022.** *To require the Comptroller General of the United States to submit to Congress a report on big tech and law enforcement, and for other purposes.* Washington: Congress, 2022. Disponível em: https://www.govinfo.gov/content/pkg/BILLS-117hr6755ih/pdf/BILLS-117hr6755ih.pdf Acessado 01/09/2023

____. House of Representative. *Digital Services Oversight and Safety Act.* **Projeto de Lei nº 6796, de 18 de fevereiro de 2022.** *To provide for the establishment of the Bureau of Digital Services Oversight and Safety within the Federal Trade Commission, and for other purposes.* Washington: Congress, 2022. Disponível em: https://www.congress.gov/117/bills/hr6796/BILLS-117hr6796ih.pdf Acessado 01/09/2023

____. House of Representative. *No Publicity for Terrorists Act.* **Projeto de Lei nº 6918, de 03 de março de 2022.** *To amend section 2339B of title 18, United States Code, to apply to social media platforms, and for other purposes.* Washington: Congress, 2022. Disponível em: https://www.congress.gov/117/bills/hr6918/BILLS-117hr6918ih.pdf Acessado 01/09/2023

____. Senate and House of Representative. *Digital Platform Commission Act.* **Projeto de Lei nº 4201/7858, de 12 de maio de 2022.** *To establish a new Federal body to provide reasonable oversight and regulation of digital platforms.* Washington: Congress, 2022. Disponível em: https://www.congress.gov/117/bills/s4201/BILLS-117s4201is.pdf Acessado 01/09/2023

____. House of Representative. *China Social Media Reciprocity Act.* **Projeto de Lei nº 8041, de 13 de junho de 2022.** *To provide authorities to prohibit the provision of services by social media platforms to individuals and entities on the Specially Designated Nationals List and certain officials and other individuals and entities of the People's Republic of China, and for other purposes.* Washington: Congress, 2022. Disponível em: https://www.congress.gov/117/bills/hr8041/BILLS-117hr8041ih.pdf Acessado 01/09/2023

____. House of Representative. *American Data Privacy and Protection Act.* **Projeto de Lei nº 8152, de 21 de junho de 2022.** *To provide consumers with foundational data privacy rights, create strong oversight mechanisms, and establish meaningful enforcement.* Washington: Congress, 2022. Disponível em: https://www.congress.gov/117/bills/hr8152/BILLS-117hr8152rh.pdf Acessado 01/09/2023

____. House of Representative. *Countering Foreign Malign Influence Act.* **Projeto de Lei nº 8409, de 18 de julho de 2022.** *To make certain modifications relating to the Social Media Data and Threat Analysis Center for the purpose of improving cooperative actions to detect and counter foreign influence operations, and for other purposes.* Washington: Congress, 2022. Disponível em: https://www.congress.gov/117/bills/hr8752/BILLS-117hr8752ih.pdf Acessado 01/09/2023

____. House of Representative. *Protecting Speech from Government Interference Act.* **Projeto de Lei nº 8752, de 30 de agosto de 2022.** *To amend title 5, United States Code, to prohibit Federal employees from advocating for censorship of viewpoints in their official capacity, and for other purposes.* Washington: Congress, 2022. Disponível em: https://www.congress.gov/117/bills/hr8409/BILLS-117hr8409ih.pdf Acessado 01/09/2023

____. House of Representative. *Block the Tok Act.* **Projeto de Lei nº 8772, de 06 de setembro de 2022.** *To establish certain requirements relating to TikTok, and for other purposes.* Washington: Congress, 2022. Disponível em: https://www.congress.gov/117/bills/hr8772/BILLS-117hr8772ih.pdf Acessado 01/09/2023

____. House of Representative. *Online Dating Safety Act.* **Projeto de Lei nº 8946, de 21 de setembro de 2022.** *To require online dating service providers to provide safety awareness and fraud ban notifications to online dating service members and to verify the identity of online dating service members, and for other purposes.* Washington: Congress, 2022. Disponível em: https://www.congress.gov/117/bills/hr8946/BILLS-117hr8946ih.pdf Acessado 01/09/2023

____. Senate. *Combating Cartels on Social Media Act.* **Projeto de Lei nº 4963, de 27 de setembro de 2022.** *To require the Secretary of Homeland Security to implement a strategy to combat the efforts of transnational criminal organizations to recruit individuals in the United States via social media platforms and other online services and assess their use of such platforms and services for illicit activities, and for other purposes.* Washington: Congress, 2022. Disponível em: https://www.congress.gov/117/bills/s4963/BILLS-117s4963is.pdf Acessado 01/09/2023

____. House of Representative. *Free Speech Defense Act.* **Projeto de Lei nº 9448, de 07 de dezembro de 2022.** *To prohibit the Federal Government from taking certain action relating to social media companies, and for other purposes.* Washington: Congress, 2022. Disponível em: https://www.congress.gov/117/bills/hr9448/BILLS-117hr9448ih.pdf Acessado 01/09/2023

____. House of Representative and Senate. *Averting the National Threat of Internet Surveillance, Oppressive Censorship, and Influence - ANTI-SOCIAL CCP Act.* **Projeto de Lei nº 9508/5245, de 13 de dezembro de 2022.** *To protect Americans from the threat posed by certain foreign adversaries using current or potential future social media companies that those foreign adversaries control to surveil Americans, learn sensitive data about Americans, or spread influence campaigns, propaganda, and censorship.* Washington: Congress, 2022. Disponível em: https://www.congress.gov/117/bills/s5245/BILLS-117s5245is.pdf Acessado 01/09/2023

UNIÃO EUROPEIA. Directiva 2011/92/UE do Parlamento Europeu e do Conselho de 13 de dezembro de 2011 relativa à avaliação dos efeitos de determinados projectos públicos e privados no ambiente. DOUE nº 26 (Serie L). **Diario Oficial de la Unión Europea** L 26, v. 2, p. 29, 2012.

UNIÃO EUROPEIA. Diretiva (UE) 2017/541 do Parlamento Europeu e do Conselho, de 15 de março de 2017, relativa à luta contra o terrorismo e que substitui a Decisão-Quadro 2002/475/JAI do Conselho e altera a Decisão 2005/671/JAI do Conselho (L 88/6). **Jornal Oficial da União Europeia-2017**. Disponível:< https://eurlex. europa. eu/legal-content/PT/TXT/PDF, 2017.

UNIÃO EUROPEIA. Diretiva (UE) 2019/790 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativa aos direitos de autor e direitos conexos no mercado único digital e que altera as Diretivas 96/9/CE e 2001/29/CE. **Jornal Oficial da União Europeia,** Luxemburgo, n. 130, p. 92125, 2019.

VALLE-CRUZ, David. *Public value of e-government services through emerging technologies.* **International Journal of Public Sector Management**, 2019.

VAN DIJCK, José. *A European perspective on platformization*. Università di Siena DISPOC, 26 abr. 2022. Disponível em: https://www.youtube.com/watch?v=Jiss8LsKwv0 Acessado em: 23/08/2022.

VAN DIJCK, José *et al.* Obsessie met data schadelik voor het goede leven. De Nieuwe Wereld, 25 jun. 2021. Disponível em: https://www.youtube.com/watch?v=ZLYhdXU3TNA&t=292s Acessado em 18/09/2022.

VAN DIJCK, José; POELL, Thomas; DE WAAL, Martijn. ***The platform society: Public values in a connective world***. Oxford University Press, 2018.

VAN DER HOF, Simone *et al. The child's right to protection against economic exploitation in the digital world*. **The International Journal of Children's Rights**, v. 28, n. 4, p. 833-859, 2020. Disponível em: https://brill.com/view/journals/chil/28/4/article-p833_833.xml Acessado em: 14/07/2023.

VIEIRA, Alessandro. PL das *Fake News*. [Entrevista concedida a Igor Rodrigues Coelho]. **Flow**, 8 mai. 2023. Disponível em: https://www.youtube.com/watch?v=nowy-UxM7fI&t=822s Acessado em: 03/06/2023.

VALENTE, Jonas. Especialistas comentam a regulação do audiovisual. **TV Senado**. 26 jul. 2021. Disponível em: https://www.youtube.com/watch?v=GpnmMGfHApw Acessado em 04/11/2023.

VIOLA, Roberto. *#EUpeople: behind the scenes with Roberto Viola*. **European Commission**. 25 jan. 2019. Disponível em: https://www.youtube.com/watch?v=P_FlxGpe_NI Acessado em 04/11/2023.

____. *Roberto Viola (DG CNECT) on digital transformation and its impact on society*. **EIT Digital**. 13 mai. 2022. Disponível em: https://www.youtube.com/watch?v=QWOoqe9tZw4 Acessado em 04/11/2023.

WANG, Ann. ***Scrutinizing Coppa: The Privacy of Our Past, Present, and Future*.** Tese de Doutorado. Joseph Wharton Scholars. Universidade da Pensilvânia. Filadélfia, EUA. 2022. Disponível em: https://repository.upenn.edu/joseph_wharton_scholars/128/ Acessado em: 15/06/2023.

WEBB, Amy; MARTINEAU, Paris. New Bill Aims to Change Algorithmic Feeds. [Entrevista concedida a Leo Laporte]. **Tech Podcast Network**, 20 fev. 2022. Disponível em: https://twit.tv/shows/this-week-in-google/episodes/651 Acessado em: 07/06/2023.

WEBER, Steven. *Data, development, and growth*. **Business and Politics**, v. 19, n. 3, p. 397-423, 2017.

WEISSMANN, Shoshana. *Online content policy: what legislative proposals aiming to rein in "big tech" need to grapple with*. **Western New England Law Review**, v. 44, n. 1, p. 35, 2022. Disponível em: https://digitalcommons.law.wne.edu/lawreview/vol44/iss1/3/ Acessado em: 19/06/2023.

WESTLING, Jeffrey. *Kids Online Safety Act Could Do More Harm Than Good*. **American Action Forum Insight**. Set. 22, 2022. Disponível em: https://www.americanactionforum.org/insight/kids-online-safety-act-could-do-more-harm-thangood/#ixzz7fcpzSq00 Acessado em: 03/06/2023.

WHITING, Zach. *Social Media Is a Harmful Product: Texas Should Prohibit Companies from Granting Access to Minors*. **Texas Public Policy Foundation**. 2023. Disponível em: https://www.texaspolicy.com/wp-content/uploads/2023/01/2023-01-RR-BTT-SocialMediaMinors-ZachWhiting.pdf Acessado em: 13/06/2023.

WOLFS, Wouter; VELDHUIS, Jan Jaap. *Regulating social media through self-regulation: a process-tracing case study of the European Commission and Facebook*. **Political Research Exchange**, v. 5, n. 1, p. 2182696, 2023.

UNIÃO EUROPEIA. Comissão Europeia. Comunicação da comissão ao parlamento europeu e ao conselho a proteção de dados. Enquanto pilar da capacitação dos cidadãos e a abordagem da UE para a transição digital - dois anos de aplicação do regulamento geral sobre a proteção de dados. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52020DC0264&from=ES Acessado em 01/08/2013.

ZHU, Guangxing. *European legislators' attitudes toward childhood sexuality from the perspective of age of consent legislation.* **European Journal of Criminology**, v. 1, p. 22, 2021. Disponível em: https://www.researchgate.net/profile/Guangxing-Zhu/publication/354832108_European_legislators'_attitudes_toward_childhood_sexuality_from_the_perspective_of_age_of_consent_legislation/links/61643fa21eb5da761e7ca3d4/European-legislators-attitudes-toward-childhood-sexuality-from-the-perspective-of-age-of-consent-legislation.pdf Acessado em:13/06/2023.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância**. Editora Intrinseca, 2021. AssembLeia Geral da ONU. (1948). "Declaração Universal dos Direitos Humanos" (217 [III] A). Paris.