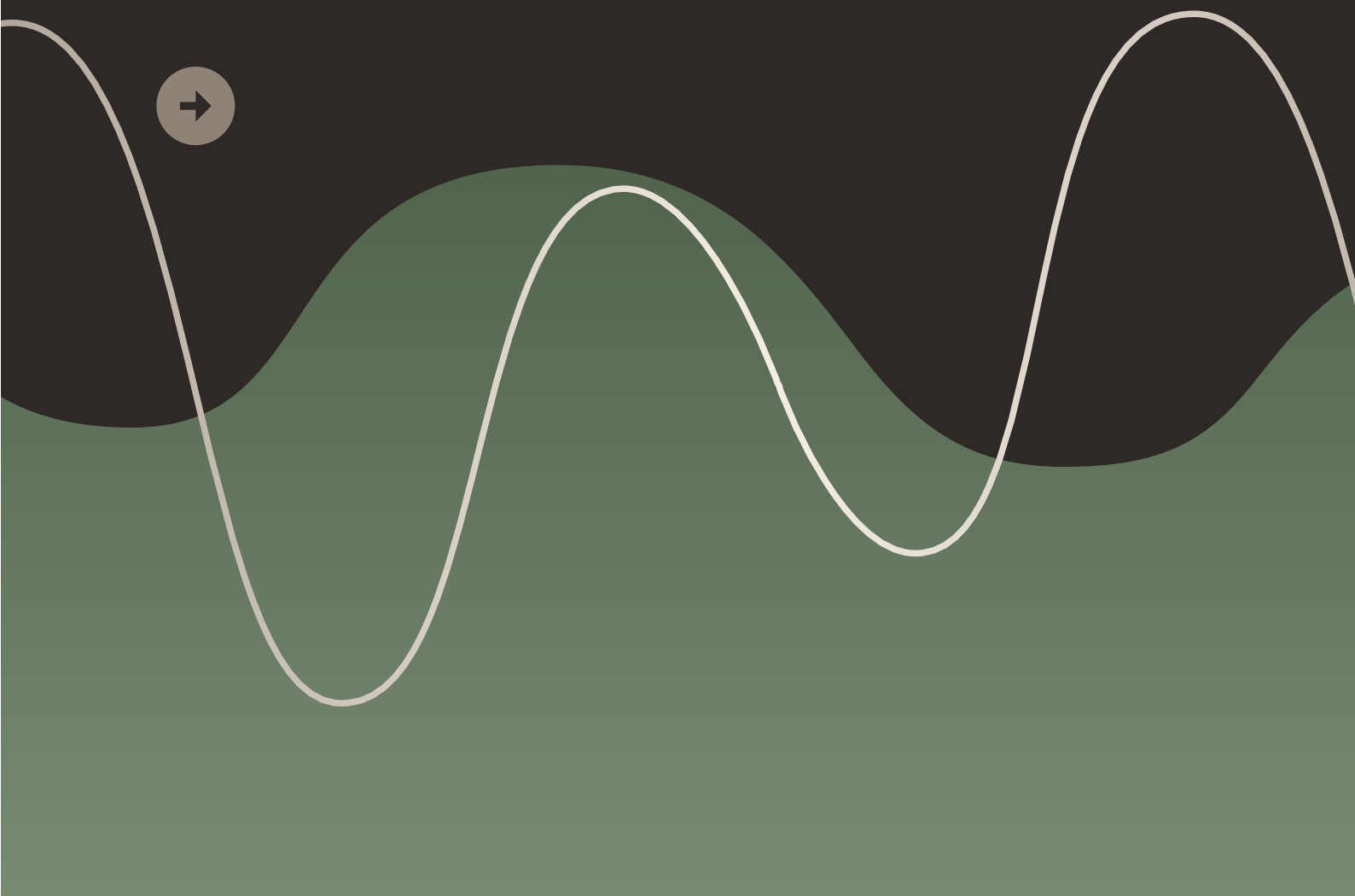


VOXIUS

Regimes de Responsabilidade por Conteúdo de Terceiros

Um estudo comparativo de diferentes jurisdições

Instituto Sivilis



VOXIUS



SIVIS

INSTITUTO SIVIS

Regimes de Responsabilidade por Conteúdo de Terceiros

Um estudo comparativo de diferentes jurisdições

NOVEMBRO | 2024



Sumário

<i>Introdução & Contextualização</i>	4
<i>Estados Unidos: Seção 230 do Communications Decency Act (CDA)</i>	6
<i>União Europeia: Diretiva de Comércio Eletrônico e a Lei de Serviços Digitais (DSA)</i>	6
<i>Reino Unido: Online Safety Act</i>	8
<i>Alemanha: NetzDG (Lei de Aplicação de Redes)</i>	9
<i>Rússia: inspirada na NetzDG, aplicada contra dissidentes</i>	10
<i>Turquia: um caso de controle político intensificado</i>	11
<i>Venezuela: controle sob o pretexto de tolerância</i>	12
<i>Cenário Brasileiro</i>	13
<i>O que o Sívris pensa?</i>	15
<i>A Elasticidade do Conceito "Manifestamente Ilícito"</i>	15
<i>A Complexidade dos Conteúdos: Entre o Preto e Branco Existe o Cinza</i>	15
<i>A Necessidade de Salvaguardas Judiciais</i>	16
<i>Riscos da Equiparação a Veículos de Comunicação</i>	16
<i>Conclusão</i>	17

Regimes de Responsabilidade por conteúdo de Terceiros

Um estudo comparativo de diferentes jurisdições

Introdução & Contextualização

A responsabilização de provedores de internet por conteúdos gerados por terceiros apresenta diferentes abordagens pelo mundo, com variáveis que refletem as características políticas e legais de cada jurisdição. Países com tradições democráticas buscam equilibrar a liberdade de expressão com a proteção de direitos fundamentais e a segurança pública. Já em regimes mais autoritários, o controle estatal sobre o conteúdo online é uma ferramenta poderosa de censura e repressão política. Este relatório busca através de um estudo comparativo compreender os diferentes regimes de responsabilidade por conteúdo de terceiros.

Nos primeiros anos da internet, os sites eram estáticos, limitando os usuários ao consumo passivo de informações. A Web 2.0 revolucionou essa dinâmica ao permitir que os próprios usuários publicassem, comentassem e compartilhassem conteúdo, com redes sociais e plataformas colaborativas como Wikipedia e YouTube. Essa nova fase, surgida no início dos anos 2000, permitiu a criação e o compartilhamento dinâmico de conteúdo, mas também trouxe questões complexas: quem é responsável por conteúdos ofensivos, difamatórios ou ilegais postados por terceiros? E se o volume de conteúdo é imenso, como monitorá-lo? Qual a responsabilidade das plataformas para impedir a circulação de conteúdos prejudiciais?

O debate sobre a responsabilidade das plataformas é complexo e amplo. Em um extremo, teríamos a isenção total de responsabilidade das plataformas; no outro, as plataformas seriam responsabilizadas por tudo que hospedam. Nenhuma dessas alternativas parece adequada para a internet atual, onde tanto usuários quanto plataformas desempenham papéis ativos.

Antes do Marco Civil da Internet (2014), o Brasil não tinha um regime jurídico específico que regulamentasse a responsabilidade das plataformas de internet por conteúdos de terceiros. A questão era interpretada com base no Código Civil, o Código de Defesa do Consumidor e na jurisprudência, o que resultava em uma abordagem imprevisível e variada. A responsabilidade das plataformas oscilava entre o modelo de responsabilidade objetiva (onde a plataforma poderia ser responsabilizada pelo simples fato de hospedar o conteúdo) e o modelo de responsabilidade subjetiva (que exigia uma análise caso a caso sobre a negligência da plataforma em monitorar e remover o conteúdo). Em alguns casos, tribunais exigiam que as plataformas monitorassem ativamente o conteúdo, e em outros, que atuassem apenas mediante denúncia ou notificação, conhecido como “notice-and-take-down”.

No sistema de “notice-and-take-down”, as plataformas são responsabilizadas pelo conteúdo dos usuários desde que fossem notificadas sobre sua suposta ilicitude. A lógica é simples: como as plataformas não podem monitorar todo o conteúdo, passariam a ser passíveis de responsabilização quando tomassem ciência do ilícito. Esse modelo, porém, mostrou-se problemático para a realidade brasileira. Pressionadas pelos advogados, as plataformas passam a remover conteúdos não por serem ilegais, mas para evitar conflitos e litígios, o *chilling effect*.

Para fortalecer a liberdade de expressão e proteger o debate público, o Congresso aprovou em 2014 o Marco Civil da Internet, que estabeleceu o modelo de responsabilidade somente após ordem judicial específica. Esse modelo preserva um equilíbrio fundamental para a democracia, especialmente em um país como o Brasil, onde a liberdade de expressão ainda carece de uma cultura de respeito. Nesse sistema, as plataformas só são responsabilizadas se, após uma decisão judicial, optarem por manter no ar o conteúdo ilegal. Casos excepcionais, como a exposição de imagens íntimas, mantêm a notificação simples para proteção rápida.

Com o julgamento da constitucionalidade do artigo 19, esse equilíbrio poderá mudar. Defensores de uma flexibilização argumentam que as plataformas não deveriam esperar uma decisão judicial para remover conteúdos que claramente violem normas de convivência social, como discursos de ódio, fraudes ao consumidor, desinformação e conteúdos prejudiciais a crianças e adolescentes. Instituições como ABERT, IDEC e Instituto Alana defendem que, nesses casos, as plataformas devem agir proativamente para proteger os usuários e impedir a circulação de informações prejudiciais.

Mais além, há ainda o risco da adoção de um modelo de responsabilização objetiva e monitoramento ativo. Esse modelo exigiria que as plataformas — sob risco de responsabilização — implementassem sistemas automatizados e equipes dedicadas para identificar e remover conteúdos considerados prejudiciais antes mesmo de qualquer notificação ou decisão judicial. Afora a inviabilidade técnica para a análise contextual das nuances interpretativas, críticos alertam que essa prática colocaria o controle da expressão pública nas mãos de *big techs*. Em países com governos autoritários, essa lógica tem sido usada para reprimir dissidências e triangular uma censura não tão disfarçada a conteúdos desinteressantes ao regime em vigor. Para o Brasil, onde o direito à expressão é ainda vulnerável, entregar esse poder a plataformas agnósticas aos interesses democráticos seria extremamente arriscado.

Para melhor compreender o cenário brasileiro, passaremos a estudar os diferentes modelos de responsabilização, desde as democracias liberais até os estados autoritários.

Estados Unidos: Seção 230 do Communications Decency Act (CDA)

Nos Estados Unidos, a Seção 230 do Communications Decency Act (CDA), de 1996, é uma das leis mais importantes para a internet moderna. Ela protege os provedores de serviços de internet contra a responsabilização pelo conteúdo gerado por terceiros. A Seção 230 é vista como uma das principais razões pelas quais plataformas como Facebook, YouTube e Twitter conseguiram crescer de forma exponencial, sem enfrentar uma enxurrada de litígios.

Princípios Fundamentais:

- **Imunidade Geral:** As plataformas não podem ser responsabilizadas por conteúdos postados por seus usuários, exceto em casos que envolvem crimes federais ou propriedade intelectual. Isso significa que, mesmo que uma plataforma hospede discurso de ódio, difamação ou desinformação, ela não será responsabilizada, a menos que esteja diretamente envolvida na criação do conteúdo.
- **Facilitador de Inovação:** A Seção 230 permite que plataformas operem sem a necessidade de monitorar preventivamente todos os conteúdos gerados pelos usuários, criando um ambiente propício à inovação e à liberdade de expressão.
- **Exceções Limitadas:** A Seção 230 não oferece imunidade em casos de crimes federais, como tráfico de drogas, violação de direitos autorais e crimes de exploração infantil.

Crítica:

Embora a Seção 230 tenha sido vital para o desenvolvimento da internet, críticos argumentam que essa ampla imunidade também possibilita a proliferação de desinformação, discurso de ódio e conteúdos prejudiciais. De todo modo, é válido destacar que, até hoje, qualquer tentativa de alterá-la ou restringir suas proteções enfrenta resistência sob o argumento de que isso prejudicaria a liberdade de expressão e sufocaria a inovação digital.

No contexto de regimes menos liberais, a Seção 230 é vista como permissiva demais, pois plataformas podem ser usadas para disseminar propaganda governamental sem nenhum tipo de responsabilização.

União Europeia: Diretiva de Comércio Eletrônico e a Lei de Serviços Digitais (DSA)

Na União Europeia, a Diretiva de Comércio Eletrônico de 2000 foi o principal marco regulatório para plataformas digitais por mais de duas décadas. Ela estabelece a isenção de responsabilidade para os intermediários online, desde que cumpram algumas condições específicas, como não terem conhecimento efetivo de conteúdos ilegais e agirem prontamente para remover o conteúdo quando notificados.

Princípios Fundamentais:

■ **Responsabilidade Condicionada ao Conhecimento:** Sob a Diretiva, as plataformas são protegidas de responsabilidade se não tiverem conhecimento dos conteúdos ilícitos hospedados em seus serviços. No entanto, uma vez que são notificadas sobre a ilegalidade do conteúdo, devem agir prontamente para removê-lo.

■ **Modelo "Notice-and-Takedown":** A diretiva introduziu um modelo de "notificação e retirada" (*notice-and-takedown*), no qual as plataformas não são obrigadas a monitorar ativamente o conteúdo, mas devem agir rapidamente quando notificadas sobre a existência de material ilegal.

■ **Proibição de Monitoramento Geral:** A diretiva proíbe a imposição de uma obrigação geral de monitoramento sobre as plataformas, ou seja, elas não são obrigadas a verificar proativamente o conteúdo antes da publicação.

Com a evolução da internet e o aumento da preocupação com a disseminação de conteúdos prejudiciais, a Lei de Serviços Digitais (DSA), em vigor desde 2023, introduziu novas obrigações específicas, particularmente para grandes plataformas digitais.

Tipos de Conteúdos Prejudiciais Abarcados pelo DSA:

■ **Desinformação Sistemática:** O DSA foca especialmente na desinformação coordenada, como campanhas de fake news em períodos eleitorais. Esse é um ponto crítico para evitar que manipulações do debate público possam influenciar resultados eleitorais.

■ **Discurso de Ódio:** O DSA exige a remoção rápida de conteúdo que incite violência ou ódio com base em características como raça, religião, gênero ou orientação sexual.

■ **Exploração Infantil:** O combate à exploração sexual infantil é tratado como prioridade, com as plataformas devendo remover imediatamente esse tipo de conteúdo ao ser identificado.

■ **Conteúdo Relacionado a Terrorismo:** O DSA introduz medidas específicas para lidar com conteúdos relacionados à promoção de atividades terroristas, exigindo sua remoção em prazos extremamente curtos.

Crítica:

Embora a DSA represente um avanço significativo na regulamentação das plataformas digitais, ela também enfrenta críticas importantes, especialmente em relação ao equilíbrio entre regulação e liberdade de expressão:

1. Risco de Sobrecarga Regulatória:

- A DSA impõe uma série de obrigações complexas e onerosas, particularmente para grandes plataformas digitais. Isso pode desencorajar a entrada de novos players no mercado e consolidar o domínio das gigantes tecnológicas, que têm mais recursos para lidar com as exigências legais e operacionais.

2. Desafios na Definição de Conteúdo Prejudicial:

- Termos como "desinformação coordenada" ou "conteúdo prejudicial" podem ser vagos e subjetivos. Isso cria um risco de interpretação excessiva, onde conteúdos legítimos podem ser erroneamente removidos por medo de penalidades regulatórias.

3. Potencial para Censura:

- Ao exigir remoções rápidas, o DSA pode induzir plataformas a erros por excesso de zelo, resultando em uma forma de censura prévia. Conteúdos controversos, mas não necessariamente ilegais, podem ser removidos em nome da conformidade com a lei, sufocando o debate público legítimo.

4. Impacto sobre a Privacidade:

- Algumas das obrigações da DSA, como a auditoria de algoritmos e o compartilhamento de dados com autoridades, levantam preocupações sobre o impacto na privacidade dos usuários e possíveis abusos por governos autoritários.

5. Risco de Fragmentação Digital:

- As exigências do DSA são específicas para a União Europeia, o que pode levar a uma fragmentação regulatória entre diferentes regiões do mundo. Isso pode dificultar a operação global de plataformas digitais, especialmente as menores, e criar barreiras para serviços internacionais.

Essas críticas refletem os desafios de encontrar um equilíbrio entre proteger os direitos dos usuários e preservar a liberdade de expressão, ao mesmo tempo em que se promove um ambiente digital seguro e inovador.

Reino Unido: Online Safety Act

O Online Safety Act, promulgado no Reino Unido em 2023, introduz um dos regimes mais abrangentes de regulamentação de conteúdo online. Essa legislação visa proteger os usuários, especialmente os mais vulneráveis, contra uma variedade de riscos no ambiente digital.

Tipos de Conteúdos Prejudiciais Abarcados:

- **Autolesão e Suicídio:** O Online Safety Act exige que as plataformas removam conteúdos que incentivem autolesão ou suicídio, um problema crescente, principalmente entre jovens.
- **Discurso de Ódio e Terrorismo:** Assim como a DSA, o Reino Unido obriga as plataformas a remover conteúdos que incitem ódio racial, religioso ou político, além de propagandas terroristas.
- **Abuso Infantil:** A lei também coloca um foco específico na remoção de conteúdos relacionados ao abuso infantil, exigindo respostas rápidas e colaboração com as autoridades.
- **Conteúdos Legais, Mas Prejudiciais:** Um aspecto único da Online Safety Act é sua cobertura de conteúdos "legais, mas prejudiciais", que, embora não infrinjam diretamente as leis, podem ter

um impacto negativo, como desinformação médica ou assédio psicológico. Isso inclui conteúdos potencialmente prejudiciais, como teorias conspiratórias que, embora não sejam ilegais, são consideradas prejudiciais à sociedade.

Crítica:

A abrangência do Online Safety Act traz preocupações significativas quanto à censura excessiva. A definição ampla de "conteúdos legais, mas prejudiciais" pode criar um ambiente onde plataformas removem preventivamente discursos controversos, incluindo debates políticos legítimos, por medo de enfrentar penalidades. Além disso, há temores de que essas normas possam ser mal utilizadas em países com menor tradição de liberdade de expressão, que veem no Online Safety Act uma justificativa para censura mais rígida sob o pretexto de proteção ao usuário.

Alemanha: NetzDG (Lei de Aplicação de Redes)

Em 2015, o Ministério da Justiça da Alemanha formou um grupo de trabalho para enfrentar o aumento de discursos de ódio e conteúdos ilegais online. Apesar de compromissos voluntários firmados com plataformas como Facebook e Twitter, uma análise de 2017 mostrou que essas iniciativas não bastavam. Isso levou à aprovação da NetzDG, em junho de 2017, que entrou em vigor em janeiro de 2018. A lei impôs obrigações rígidas para plataformas com mais de dois milhões de usuários, exigindo a remoção de conteúdos "manifestamente ilegais" em até 24 horas ou sete dias, dependendo da complexidade. Multas de até 50 milhões de euros foram estabelecidas para descumprimentos.

A NetzDG gerou debates intensos. Defensores destacaram sua importância para combater discursos de ódio e proteger vítimas, enquanto críticos apontaram riscos de remoções excessivas, falta de supervisão judicial e incentivos para censura preventiva. Casos como a remoção de um comentário da deputada Beatrix von Storch e a suspensão da conta do ativista Mike Samuel Delberg evidenciaram os dilemas da lei. Ao mesmo tempo, sua implementação inspirou governos autoritários, como Rússia e Turquia, a criar legislações próprias de controle de conteúdo, intensificando preocupações sobre a instrumentalização de sua abordagem.

A experiência alemã oferece lições importantes sobre os desafios de equilibrar liberdade de expressão e proteção contra abusos em democracias, especialmente no contexto de plataformas digitais globais.

Princípios Fundamentais:

- **Remoção Rápida de Conteúdos Ilegais:** A NetzDG exige que plataformas removam conteúdos claramente ilegais, como incitação ao ódio, no prazo de 24 horas após a notificação. Em casos mais complexos, as plataformas têm até sete dias para remover o conteúdo.
- **Multas Significativas:** O não cumprimento pode resultar em multas de até 50 milhões de euros para a plataforma, uma das penalidades mais rigorosas do mundo.

■ **Discurso de Ódio e Terrorismo:** A lei foca principalmente na remoção de conteúdos extremistas, como discursos de ódio racista e propaganda terrorista.

Crítica:

A NetzDG tem sido criticada por incentivar a censura privada em massa. Plataformas, com medo das multas, muitas vezes removem conteúdos antes de avaliar cuidadosamente sua legalidade, o que pode prejudicar a liberdade de expressão. Além disso, a NetzDG foi vista como um modelo por regimes autoritários, como a Rússia e a Turquia, que implementaram legislações semelhantes sob o pretexto de proteger a ordem pública, mas com o objetivo de controlar o discurso político e suprimir dissidência.

Rússia: inspirada na NetzDG, aplicada contra dissidentes

A experiência da Rússia com a adaptação de uma legislação inspirada no modelo alemão, especialmente a NetzDG, oferece lições valiosas para o debate sobre o regime de responsabilidade das plataformas no Brasil.

Em 2017, o governo russo apresentou uma lei que exigia que plataformas de redes sociais com mais de dois milhões de usuários removessem conteúdos considerados "ilegais". Apesar de o modelo alemão ter sido desenvolvido em um contexto democrático para lidar com discurso de ódio, na Rússia, a implementação foi rapidamente apropriada como ferramenta de controle estatal.

Com prazos rígidos para remoção de conteúdos e definições vagas sobre o que constitui material ilegal, a legislação russa estabeleceu as bases para um regime de censura digital intensificada. A organização Repórteres Sem Fronteiras (RSF) criticou a proposta russa como uma cópia direta da NetzDG, mas com o objetivo de limitar o debate público e reforçar a repressão a vozes dissidentes. A lei, implementada com severas sanções financeiras, tornou as plataformas digitais agentes involuntários do controle estatal, com as consequências sendo sentidas por jornalistas, ativistas e cidadãos comuns.

Nos anos que se seguiram, a Rússia expandiu seu arcabouço de leis repressivas. Em 2019, medidas como as leis No.31-FZ e No.27-FZ conferiram ao Roskomnadzor, a agência estatal de supervisão de comunicações, o poder de bloquear conteúdo online considerado "não confiável". A pandemia de COVID-19 acelerou a tendência, com novas regulamentações criminalizando a disseminação de informações que contradissem as versões oficiais. Em 2022, a invasão da Ucrânia trouxe um novo patamar de repressão, com leis impondo penas de até 15 anos de prisão para quem divulgasse "informações falsas" sobre as ações das Forças Armadas Russas.

A trajetória russa destaca o risco de legislações como a NetzDG, quando transplantadas para contextos autoritários, se transformarem em instrumentos de controle e censura, contrariando os princípios democráticos de liberdade de expressão.

Princípios Fundamentais:

- **Obrigação de Remoção de Conteúdos em 24 Horas:** Assim como a NetzDG, a lei russa exigia a remoção de conteúdos ilegais em prazos rígidos, mas com definições amplamente vagas sobre o que era considerado "ilegal".
- **Sanções Financeiras Severas:** Penalidades significativas incentivaram a autocensura das plataformas, que preferiam remover conteúdos de forma preventiva.
- **Controle Estatal Intensificado:** A Roskomnadzor, agência estatal de comunicações, recebeu amplos poderes para bloquear conteúdos, expandindo o monitoramento da esfera digital.

Crítica:

A implementação da legislação marcou o início de uma série de restrições. Em 2019, novas leis conferiram à Roskomnadzor a capacidade de bloquear conteúdos classificados como "não confiáveis". Durante a pandemia de COVID-19, regulamentações adicionais criminalizaram a disseminação de informações contrárias às versões oficiais sobre crises sanitárias. Em 2022, com a invasão da Ucrânia, leis ainda mais severas impuseram penas de até 15 anos de prisão para quem divulgasse "informações falsas" sobre as Forças Armadas Russas.

A adaptação russa da NetzDG evidenciou o risco de legislações originalmente democráticas serem apropriadas para fins autoritários. Jornalistas, ativistas e cidadãos comuns foram diretamente afetados, enfrentando censura digital e restrições às liberdades de expressão. O modelo russo subverteu o princípio democrático que orientava a legislação alemã, transformando-o em ferramenta de controle político e repressão a dissidentes.

Turquia: um caso de controle político intensificado

A Turquia, nos últimos anos, consolidou-se como um exemplo notório de como legislações destinadas a regulamentar o discurso online podem ser adaptadas para reforçar o controle político. Inspirando-se em parte no modelo da NetzDG alemã, o governo turco implementou, em 2020, uma série de medidas que ampliaram a vigilância sobre o ambiente digital e reforçaram a censura estatal.

Desde sua implementação, a lei turca serviu como um instrumento poderoso para o governo do presidente Recep Tayyip Erdoğan consolidar seu controle sobre o espaço público. Sob o pretexto de combater o discurso de ódio e a desinformação, as autoridades passaram a monitorar, restringir e remover conteúdos que criticassem o governo ou questionassem políticas estatais. Jornalistas, ativistas e membros da oposição foram frequentemente alvos dessa legislação.

A legislação turca foi amplamente utilizada durante períodos eleitorais, como em 2023, para limitar o alcance de figuras proeminentes da oposição. Um caso emblemático envolveu o líder da oposição Kemal Kılıçdaroğlu, acusado de espalhar fake news após criticar políticas governamentais. Além disso, a lei foi usada para silenciar vozes críticas em plataformas como Twitter e Facebook,

forçando as empresas a cumprir ordens de remoção de conteúdos sob ameaça de penalidades severas.

Princípios Fundamentais:

- **Remoção de Conteúdos “Ilegais”:** Assim como a NetzDG, a legislação turca exige que plataformas de redes sociais removam conteúdos classificados como “ilegais”. No entanto, os critérios para tal classificação são amplos e muitas vezes ambíguos, incluindo acusações como disseminação de “desinformação” ou conteúdos que prejudiquem “a ordem pública”.
- **Exigências de Dados Locais:** Penalidades As plataformas foram obrigadas a estabelecer representações legais no país e armazenar dados dos usuários localmente, facilitando o acesso governamental a essas informações.
- **Multas e Restrições:** Empresas que não cumprissem as exigências da nova legislação enfrentariam sanções financeiras severas, restrições de largura de banda e até a proibição total de operar no país.

Crítica:

Organizações de direitos humanos e liberdade de imprensa denunciaram o modelo turco como um exemplo extremo de censura digital. A Human Rights Watch e o Comitê para a Proteção dos Jornalistas destacaram como a aplicação da lei turca exacerbou o ambiente de autocensura e deteriorou ainda mais a liberdade de expressão no país.

Enquanto o governo defendia a legislação como uma medida necessária para proteger a segurança nacional e a ordem pública, críticos apontaram para seu uso deliberado como uma ferramenta de repressão política. A exigência de que as plataformas compartilhassem dados dos usuários também levantou preocupações significativas sobre privacidade e vigilância estatal.

Venezuela: controle sob o pretexto de tolerância

A experiência venezuelana com a regulamentação de conteúdos online destaca como legislações direcionadas a combater o discurso de ódio podem ser instrumentalizadas para silenciar dissidentes e reforçar regimes autoritários. Em 2017, o governo de Nicolás Maduro promulgou a Lei contra o Ódio, pela Coexistência Pacífica e Tolerância, um marco legislativo que, ostensivamente, visava promover a harmonia social, mas que, na prática, ampliou os mecanismos de censura e repressão no país.

Princípios Fundamentais:

- **Sanções Severas:** A legislação estabelece penas de até 20 anos de prisão para quem for acusado de disseminar discurso de ódio, além de multas e outras penalidades administrativas.

■ **Definições Ambíguas:** O texto da lei adota definições vagas sobre o que constitui "discurso de ódio", abrindo margem para interpretações amplas e subjetivas, geralmente orientadas para proteger os interesses do governo.

■ **Obrigação de Remoção de Conteúdos:** As plataformas e emissoras de mídia são obrigadas a remover conteúdos considerados ofensivos ou ameaçadores em prazos determinados, sob pena de sanções legais.

Crítica:

Organizações internacionais, como a Human Rights Watch e o Comitê para a Proteção dos Jornalistas, condenaram a Lei contra o Ódio como um instrumento de censura e repressão política. Essas entidades destacam que a lei venezuelana viola os princípios fundamentais de liberdade de expressão e acesso à informação, contribuindo para a deterioração das instituições democráticas no país.

Desde sua implementação, a Lei contra o Ódio tem sido utilizada como uma ferramenta para silenciar vozes críticas ao governo. Jornalistas, ativistas e membros da oposição frequentemente se tornam alvos de investigações e prisões arbitrárias, sob a acusação de incitar ódio ou desestabilizar a ordem pública.

Um exemplo emblemático foi o caso do jornalista Jesús Medina Ezaine, preso por reportar sobre a crise humanitária nos hospitais venezuelanos. Ele foi mantido em detenção por 16 meses, sem julgamento, acusado de incitar ódio por meio de suas reportagens. Este e outros episódios demonstram como a lei é empregada seletivamente para perseguir aqueles que expõem a realidade do país ou criticam o regime de Maduro.

Além disso, a legislação tem impactado profundamente a liberdade de imprensa e o acesso à informação no país. Sob o pretexto de regular discursos prejudiciais, o governo consolidou um controle quase total sobre o espaço digital e midiático, restringindo drasticamente o debate público e a diversidade de opiniões.

Cenário Brasileiro

O artigo 19 do Marco Civil da Internet está em pauta no Supremo Tribunal Federal (STF) para julgamento de sua constitucionalidade. Esse artigo é um dos pilares da regulamentação da internet no Brasil, pois trata diretamente da responsabilidade civil dos provedores de aplicações de internet (como Facebook, Google, TikTok, Kwai, mas também de marketplaces como o Mercado Livre) por conteúdos gerados por terceiros.

Em linhas gerais, o artigo 19 estabelece que os provedores de internet só podem ser civilmente responsabilizados por danos decorrentes de conteúdo gerado por terceiros se, após uma ordem judicial específica, não tomarem as providências necessárias para remover o conteúdo considerado ilegal. Isso garante que as plataformas não sejam responsabilizadas de maneira automática ou preventiva, preservando a liberdade de expressão.

Dois processos principais, que tratam diretamente da regulamentação e do papel das empresas de tecnologia na moderação de conteúdo, estão pautados para julgamento conjunto, com potencial impacto em toda a infraestrutura de governança da internet no país.

Esses processos são dois Recursos Extraordinários (RE) de repercussão geral que levantam discussões sobre a constitucionalidade de dispositivos do Marco Civil e sobre a responsabilidade das plataformas no controle de conteúdos prejudiciais. Abaixo, um resumo das ações:

- **RE 1.037.396 (Tema 987) – Relator: Ministro Dias Toffoli**

O caso discute a constitucionalidade do artigo 19 do Marco Civil da Internet, que prevê a necessidade de uma **ordem judicial específica para responsabilizar plataformas digitais pelo conteúdo postado por terceiros**. O debate gira em torno de saber se essa exigência está em conformidade com a Constituição.

- **RE 1.057.258 (Tema 533) – Relator: Ministro Luiz Fux**

Trata da possibilidade de as plataformas serem **responsabilizadas por conteúdos gerados por usuários sem uma ordem judicial, a partir de uma simples notificação extrajudicial**. A ação questiona a viabilidade de remover **conteúdos ofensivos ou que promovam ódio ou desinformação sob essa condição**.

Esses julgamentos podem redefinir o papel das plataformas digitais no Brasil, estabelecendo novos parâmetros para a responsabilização das empresas pelo conteúdo gerado por seus usuários, em um cenário onde a internet tem uma influência crescente sobre a disseminação de informações e a formação de opiniões.

O que o Sivis pensa?

No Instituto Sivis, nosso compromisso com uma sociedade mais colaborativa, democrática e livre nos leva a avaliar com cautela as implicações do julgamento da constitucionalidade do artigo 19 do Marco Civil da Internet.

A eventual introdução – inspirada no modelo da NETZDG – de uma responsabilidade solidária para os provedores de internet, sem a necessidade de uma ordem judicial, quando o conteúdo for considerado "manifestamente ilícito", suscita preocupações profundas. A falta de clareza e a porosidade desse conceito abrem precedentes perigosos para a liberdade de expressão no contexto brasileiro, permitindo interpretações amplas e subjetivas que podem restringir o debate público.

A Elasticidade do Conceito "Manifestamente Ilícito"

O termo "**manifestamente ilícito**" é inerentemente flexível, variando conforme o contexto político e social, o que pode gerar remoções injustificadas de conteúdos. Em teoria, esse conceito deveria se aplicar a conteúdos claramente ilegais, como a incitação ao terrorismo ou à violência. No entanto, em muitos casos práticos, essa classificação é matizada, e o que pode ser visto como uma "**ameaça à ordem pública**" em um contexto pode, em outro, ser uma crítica política legítima. Países como Rússia e China oferecem exemplos claros de como o controle sobre a internet pode ser distorcido para silenciar opositores sob o pretexto de proteger a ordem pública. Nessas jurisdições, discursos críticos ao governo frequentemente são rotulados como "fake news" ou "ameaças à segurança nacional", justificando sua remoção e promovendo a censura.

Ao introduzir a responsabilidade dos provedores sem a mediação judicial, corremos o risco de adotar um modelo de censura privada no Brasil. A NetzDG alemã, embora tenha o objetivo de combater discursos de ódio e extremismo, criou um ambiente em que as plataformas removem preventivamente conteúdos ambíguos, muitas vezes eliminando debates legítimos por medo de serem multadas. Isso exemplifica o risco de colocar nas mãos de plataformas privadas o poder de definir o que é aceitável no espaço público digital.

A Complexidade dos Conteúdos: Entre o Preto e Branco Existe o Cinza

A análise de conteúdos pela inteligência artificial (IA) tem sido apontada como uma solução eficiente para lidar com grandes volumes de dados. De fato, em casos de conteúdos que são binários, como a pornografia infantil, a IA pode atuar de forma precisa e permitir uma atuação célere das plataformas. A identificação de conteúdos desse tipo é objetiva: ou existe, ou não existe, e as tecnologias automatizadas, como hashes de imagens já catalogadas, são eficazes para removê-los. Nesses casos, a remoção imediata não suscita preocupações quanto à liberdade de expressão, já que se trata de um ilícito claro e universalmente condenado.

Porém, o cenário muda quando tratamos de conteúdos que exigem uma análise contextual mais refinada. Um discurso político hiperbólico, por exemplo, pode ser facilmente confundido com incitação à violência ou à desordem, dependendo de quem o interpreta. A retórica inflamada é uma característica comum em tempos de polarização política, e discursos que desafiam o status quo

podem ser mal interpretados como atentados à democracia. Nesse contexto, algoritmos de moderação automatizada falham ao lidar com nuances, removendo conteúdos que, apesar de controversos, são legítimos dentro de um debate democrático.

Esse tipo de conteúdo não pode ser tratado de forma binária. Ao permitir a responsabilização dos provedores sem uma revisão judicial, criamos um ambiente em que as plataformas, para evitar litígios e penalidades, optam por remover qualquer conteúdo que possa ser mal interpretado, sufocando a liberdade de expressão e prejudicando a pluralidade de vozes no debate público.

A Necessidade de Salvaguardas Judiciais

Ao diferenciarmos conteúdos binários, como pornografia infantil, de conteúdos matizados, como discursos políticos, fica evidente a importância de garantir que a remoção de conteúdos complexos ocorra **com base em uma manifestação do Estado-Juiz** e não através da delegação às plataformas da subsunção dos fatos à norma. O papel da justiça é justamente o de ponderar os direitos em conflito, garantindo que a remoção de conteúdos seja feita de forma criteriosa, evitando censura arbitrária e assegurando que as **plataformas não se tornem árbitros do que pode ou não ser dito**.

A experiência internacional mostra que, sem salvaguardas claras, regulamentações sobre conteúdo podem ser usadas indevidamente para suprimir o debate político e silenciar vozes dissidentes. Se o Brasil não implementar medidas de proteção adequadas, **corremos o risco de seguir exemplos preocupantes**, como os de Rússia e Turquia, onde leis de controle de conteúdo são rotineiramente utilizadas para reprimir a dissidência.

Riscos da Equiparação a Veículos de Comunicação

A equiparação entre plataformas e veículos de comunicação para anúncios pagos cria uma exigência de que as plataformas sejam responsáveis por todos os anúncios publicados, o que pode levar a um comportamento de censura preventiva. A fim de evitar riscos legais, as plataformas podem acabar rejeitando anúncios legítimos, mas que envolvem temas controversos ou críticos ao poder, limitando o alcance de vozes dissidentes ou de movimentos sociais. Esse cenário já foi observado em legislações rígidas como a NetzDG na Alemanha, onde o medo de sanções pesadas levou as plataformas a adotarem uma política de remoção excessiva de conteúdos, incluindo anúncios de caráter político ou social.

Além disso, tal equiparação desconsidera a natureza descentralizada e colaborativa das plataformas digitais. Diferentemente dos veículos de mídia, onde o controle editorial é absoluto, as plataformas funcionam como intermediárias que possibilitam a veiculação de anúncios de terceiros. Impor uma responsabilidade direta sobre esses anúncios, como se as plataformas fossem responsáveis pelo conteúdo dos mesmos, ignora a diferença crucial no funcionamento desses dois tipos de mídia. Isso pode, inclusive, aumentar os custos de operação dessas plataformas, criando barreiras de entrada para novas empresas e prejudicando a inovação tecnológica.

Outro ponto a ser destacado é o impacto negativo que essa equiparação pode ter sobre a pluralidade de ideias. No atual cenário digital, os anúncios pagos são um dos principais meios de disseminação de informação, e a equiparação com veículos de mídia tradicionais pode inibir a publicação de anúncios críticos ao governo ou a instituições poderosas, uma vez que as plataformas, temendo responsabilizações legais, optariam por bloquear preventivamente qualquer conteúdo considerado minimamente arriscado.

Conclusão

Portanto, no Instituto Sivis, vemos com preocupação essa tentativa de equiparar plataformas de internet a veículos de comunicação no contexto de anúncios pagos. Enquanto entendemos a necessidade de responsabilizar as plataformas por conteúdos claramente ilícitos, é crucial que essa responsabilidade seja aplicada de forma proporcional e que questões mais matizadas, como anúncios com teor político ou social, sejam tratadas com uma abordagem mais cuidadosa. A intervenção judicial continua sendo essencial nesses casos, para que as plataformas não sejam forçadas a adotar políticas de remoção preventiva que limitem a liberdade de expressão e a diversidade de ideias.

No Instituto Sivis, defendemos uma abordagem que preserve a liberdade de expressão, assegurando que a remoção de conteúdos ocorra de maneira justa, transparente e sujeita ao controle judicial, evitando excessos e garantindo um ambiente democrático vibrante e plural.

Visão geral do Sivis para aprimoramento da responsabilidade por conteúdo de terceiros no Brasil

- 1) Defendemos o atual modelo de regime de responsabilidade previsto nos artigos 19 e 21 do Marco Civil da Internet.
- 2) Conforme aprendido com os modelos alemão, russo e turco, é perigoso implementar um dever de monitoramento e ação proativa das plataformas, sob o risco de se triangular a censura quando se transfere a responsabilidade para as plataformas.
- 3) É delicada ampliação do rol do artigo 21, uma vez que, ao se colocar conteúdos políticos controversos como discurso de ódio, abre-se para o risco de censura privada.
- 4) É possível criar medidas intermediárias como notificações do ministério público ou polícia em casos de risco iminente à vida. No entanto, deve-se garantir sempre o maior grau possível de transparência, para que não haja risco de influência de agentes governamentais no discurso público.



Rua Mauricio Caillet, 47
80250-110 / Curitiba, PR

WWW.SIVIS.ORG.BR