

LIBERDADE DE EXPRESSÃO E VIOLÊNCIA POLÍTICA DE GÊNERO E RAÇA NAS REDES SOCIAIS



Coordenação: Prof^ª. Dr^ª. Yasmin Curzi

Supervisão e edição: Giullia Thomaz

Pesquisadores: Alice Amorim, Ana Clara Conde, Catherine Rodrigues, Gabriel Sobral, Gabriela Braga, Pandora Verbicário, Luisa Aquino, Lais Jardim, Maria Clara Vendas e Thiago Gobira

Revisão: Lorena Abbas e Idalie Brossard

Data da Publicação: Fevereiro de 2024

Como citar este material:

CURZI, Y., THOMAZ, G., AMORIM, A., AQUINO, L., CONDE, A. C., RODRIGUES, C., SOBRAL, G., BRAGA, G., VERBICÁRIO, P., JARDIM, L., VENDAS, M. C., GOBIRA, T. *Liberdade de Expressão e Violência Política de Gênero e Raça nas Redes Sociais. Digital Safety Program*, FGV Direito Rio, 2024.

Dados Internacionais de Catalogação na Publicação (CIP)
Ficha catalográfica elaborada pela Biblioteca Mario Henrique Simonsen/FGV

Liberdade de expressão e violência política de gênero e raça nas redes sociais / Yasmin Curzi (coord.). - Rio de Janeiro : FGV Direito Rio, 2024. 76 p. : il.

Inclui bibliografia.
ISBN 978-65-86060-60-7

1. Liberdade de expressão. 2. Direitos fundamentais. 3. Redes sociais online – Aspectos sociais. 4. Discriminação racial. I. Curzi, Yasmin. II. Escola de Direito do Rio de Janeiro da Fundação Getúlio Vargas.

CDD – 341.27

Elaborada por Márcia Nunes Bacha – CRB-7/4403

Este material, seus resultados e conclusões são de responsabilidade dos autores e não representam, de qualquer maneira, a posição institucional da Fundação Getúlio Vargas / FGV Direito Rio.

Apoio:

Sumário

Lista de Abreviações	6
1. Apresentação	8
1.1 Pesquisadores	10
1.2 Coordenação e supervisão	12
1.3 Revisão	13
2. Olhar interseccional para a tecnologia	14
2.1 Violência de Gênero Facilitada pela Tecnologia (TFGBV)	15
2.2 Glossário de TFGBV	16
3. Censura na Internet	20
3.1 Como o Estado regula a expressão online?	21
3.2 Como a censura privada acontece nas redes sociais?	24
<i>Shadowbanning</i>	26
<i>Denúncia coordenada</i>	27
Caso 1. A Censura à Lola Aronovich	28
Caso 2. O Hackeamento de Janja da Silva	30

O papel das plataformas na segurança de seus usuários	31
3.3 Como posso recorrer de censura privada?	32
4. Crimes de ódio online	34
4.1 Contexto legislativo sobre crimes de ódio no Brasil	36
Caso 3. Ataques à Érika Hilton	37
4.2 Como recorrer quando sofro crimes de ódio nas redes? ----	38
4.3 Qualquer um pode ser vítima de discurso de ódio?	40
5. Ameaças à integridade psicofísica nas redes	42
5.1 A Lei de Stalking	44
5.2 Como agir quando acredito que estou sendo vítima de <i>stalking</i> ou ameaça?	46
6. Privacidade, honra e imagem na Era Digital	48
6.1 Quais são meus direitos quanto à minha imagem e honra? -	50
6.2 Imagens íntimas não consentidas	51
6.3 Quando a misoginia encontra a IA: deep fakes e deep nudes	53

Caso 4. Deep nudes e violência política de gênero e raça contra Diane Rwigara	54
6.4 Como lidar com a disseminação de imagens íntimas produzidas por IA?	55
6.5 Desinformação generificada e violência política	56
Caso 5. Manuela d'Ávila e campanhas de desinformação generificada	58
7. Recomendações para o setor público	59
8. Recomendações para o setor privado	63
9. Considerações finais	65
Referências bibliográficas	67
Outros materiais relevantes	76



Lista de siglas e abreviações

ABIN	Agência Brasileira de Inteligência
CTS	Centro de Tecnologia e Sociedade
DEAM	Delegacia de Atendimento à Mulher
DECRADI	Delegacia de Crimes Raciais e Delitos de Intolerância
DDoS	Distributed Denial of Service
DSA	Digital Services Act
DSP	Digital Safety Program
FGV	Fundação Getulio Vargas
IA	Inteligência Artificial
LGBTQIA+	Lésbicas, gays, bissexuais, transsexuais, queer, intersexo, assexual e outros
LGPD	Lei Geral de Proteção de Dados
MCI	Marco Civil da Internet
ONU	Organização das Nações Unidas

PD&I	Programa de Diversidade & Inclusão
PL	Projeto de Lei
PT	Partido dos Trabalhadores
PV	Partido Verde
SECOM	Secretaria de Comunicação Social
SENASP	Secretaria Nacional de Segurança Pública
TFGBV	Tech-Facilitated Gender-Based Violence
UNESCO	Organização das Nações Unidas para a Educação, a Ciência e a Cultura
UNGP	United Nations Guiding Principles on Business and Human Rights
VPN	Virtual Private Network

1. Apresentação

O **Digital Safety Program (DSP)** é um projeto de extensão, desenvolvido na **FGV Direito Rio**, voltado para promover o engajamento de discentes da graduação em questões localizadas na interseção entre tecnologia e direitos humanos. Sua essência reside na promoção de um ambiente de aprendizado interativo e colaborativo, incentivando os participantes a explorar, analisar e contribuir para a segurança digital.

A partir de encontros semanais com pesquisadoras do **Programa de Diversidade & Inclusão (PD&I)** e do **Centro de Tecnologia e Sociedade (CTS)** da FGV Direito Rio, a segurança digital é debatida não apenas como um conjunto de práticas destinadas a proteger a integridade de informações, mas também como um conceito ampliado que abrange a necessidade de proteção e promoção de direitos humanos no ambiente digital. De tal modo, o DSP inclui, mas não se restringe a, debates de questões de privacidade, liberdade de expressão, acesso à informação e proteção contra formas digitais de violência e discriminação.

O DSP adota uma abordagem interseccional e multidisciplinar, reconhecendo que os desafios da segurança digital não podem ser plenamente compreendidos ou resolvidos sem considerar a interação complexa entre tecnologia, sociedade, cultura, política e economia. Buscamos promover a compreensão de que as questões de segurança digital são intrinsecamente ligadas a contextos mais amplos de desigualdade, poder e justiça social.

A presente publicação tem como o objetivo trazer luz ao debate sobre liberdade de expressão e violência política de gênero e raça nas redes sociais. Inspirada em trabalhos anteriores, como InternetLab e Coding Rights (2017), ela busca atualizar casos atinentes a tais temáticas, com o objetivo de servir como um material de apoio a todas as pessoas interessadas em saber mais sobre seus direitos no contexto digital.

O texto pode ser utilizado como um guia para auxiliar pessoas vítimas de violência política de gênero e raça online, assessorias jurídicas ou de comunicação de candidatas(os) a cargos eletivos, profissionais do Direito e outras áreas do conhecimento, entre outros.



1.1 Pesquisadores do DSP

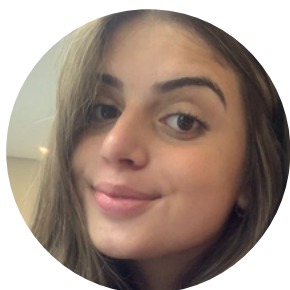
Alice Amorim

Aluna do 6º período da FGV Direito Rio, estagiária no Braz, Coelho, Veras, Lessa, Bueno e integrante do grupo de estudos Digital Safety



Ana Clara Conde

Aluna do 4º período da FGV Direito Rio, pesquisadora voluntária no projeto "Observatório do Sistema de Justiça Criminal", monitora das disciplinas "Crime e Sociedade" e "Penas e Medidas Alternativas" e integrante do grupo de estudos Digital Safety



Catherine Rodrigues

Aluna do 2º período da FGV Direito Rio, Integrante da Liga Acadêmica de Ciências Criminais de Graduandos da FGV Direito Rio e integrante do grupo de estudos Digital Safety.



Gabriel Sobral

Aluno do 2º período da FGV Direito Rio, Diretor Acadêmico da Liga de Análise Econômica do Direito e integrante do grupo de estudos Digital Safety



Gabriela Braga

Aluna do 2º período da FGV Direito Rio, membro da Liga Estudantil de Direito Constitucional (LEDC) e do Núcleo de Mediação e Negociação (NMN) e integrante do grupo de estudos Digital Safety



Pandora Verbicário

Aluna do 8º período da FGV Direito Rio, pesquisadora voluntária do Centro de Tecnologia e Sociedade (CTS-FGV) e do Centro de Justiça e Sociedade (CJUS-FGV) e integrante do grupo de estudos Digital Safety.



Maria Clara Vendas

Aluna do 7º Período de Direito na FGV, estagiária do Maneira Advogados e integrante do grupo de estudos Digital Safety.

Lais Jardim

Aluna do 6º período direito da Fundação Getúlio, estagiária do Maneira Advogados e integrante do grupo de estudos Digital Safety.



Luisa Aquino

Aluna do 8º período da FGV Direito Rio, Estagiária de Propriedade Intelectual e Direito Digital do Tauil e Chequer, presidente da liga estudantil de propriedade intelectual (LEPI), intercambista na universidade NOVA de Lisboa e integrante do grupo de estudos Digital Safety.

Thiago Gobira

Aluno do 6º período na FGV Direito Rio e integrante do grupo de estudos Digital Safety.



1.2 Coordenação e supervisão

Yasmin Curzi

Advogada, professora da FGV Direito Rio, doutora em Sociologia pelo Instituto de Estudos Sociais e Políticos (IESP-UERJ) e mestre em Sociologia pela Pontifícia Universidade Católica do Rio de Janeiro (PUC - Rio). Coordenadora do Programa Diversidade e Inclusão da FGV Direito Rio e pesquisadora no Centro de Tecnologia e Sociedade (CTS-FGV)



Giullia Thomaz

Internacionalista, mestranda em sociologia e antropologia pelo Instituto de Filosofia e Ciências Sociais (IFCS - UFRJ), pesquisadora no Centro de Tecnologia e Sociedade (CTS-FGV) e no Programa Diversidade e Inclusão (PD&I) da FGV.

1.3 Revisão

Lorena Abbas

Doutoranda em Políticas Públicas, Estratégias e Desenvolvimento (PPED/IE/UFRJ). Mestre e graduada em Direito pela Universidade Federal de Juiz de Fora (UFJF/MG). Pesquisadora do Programa de Diversidade & Inclusão (PD&I) da Escola de Direito da Fundação Getúlio Vargas (FGV Direito Rio), atuando no projeto "Mídia e Democracia" (2023-25), apoiado pela União Europeia. No âmbito do PD&I desenvolve atividades acadêmicas em assuntos relacionados à interseção entre tecnologia e direitos humanos.



Idalie Brossard

Graduanda em Ciências Sociais pela Fundação Getúlio Vargas-RJ (CPDOC/FGV). É estagiária do Programa de Diversidade & Inclusão da Escola de Direito da Fundação Getúlio Vargas (FGV Direito Rio). Trabalhou na Fondation Good Planet (Paris, França) com bolsa do governo francês e em algumas ONGs como estagiária, incluindo Gastromotiva (Rio de Janeiro) e a Escola de Sustentabilidade Integral (Salvador, Bahia).



2. Olhar interseccional para a tecnologia

Para a produção desta publicação, os esforços de pesquisa do **Digital Safety Program (DSP)** se deram no sentido de investigar em qual medida as tecnologias permitem a amplificação de violações a direitos fundamentais além de novas formas de violação. Compreendendo que as violências online refletem estruturas de desigualdades sociais mais amplas, como de gênero, raça e classe, pensamos tal temática a partir de termos **interseccionais**. De tal modo, levamos em conta a diferença de grau e tipo de violência que sofrem mulheres, pessoas negras, pardas, indígenas e quilombolas, trans, não-binárias e integrantes da comunidade LGBTQIA+ de maneira geral, em relação a outros grupos sociais.

Nesse sentido, esta publicação procura trazer luz a casos paradigmáticos de **discurso de ódio** e **violações a direitos** de usuários que integram grupos sociopoliticamente minorizados, praticadas por outros usuários ou pelas próprias plataformas de redes sociais. Compreendendo que o espaço digital é essencial para a comunicação em massa e especialmente fundamental para a formação de redes de solidariedade, mobilização e engajamento de tais grupos, partimos da literatura especializada sobre liberdade de expressão e violência online para a identificação de condutas que ameaçam a concretização de seus direitos fundamentais.

Procuramos elucidar terminologias específicas do campo de estudos digitais sobre fenômenos e condutas atinentes a tais temáticas. Para isso, a presente publicação se divide em 7 capítulos, abordando a violência de gênero facilitada pela tecnologia em forma de glossário, trazendo para o debate casos específicos, legislações vigentes e recomendações práticas.

2.1 Violência de Gênero Facilitada pela Tecnologia (TFGBV)

A definição de “*Technology-Facilitated Gender-Based Violence*”, ou TFGBV, é a maneira pela qual segmentos da literatura especializada em estudos de gênero e tecnologia têm categorizado práticas e formas de discriminação e violência de gênero a partir do uso de tecnologias, dentre elas, a rede mundial de computadores e aplicações da Internet. Serve para categorizar as **violências que se valem do uso de ferramentas digitais para perpetrar a intolerância contra mulheres e pessoas LGBTQIA+**.

Algumas das principais condutas são detalhadas na tabela abaixo, construída a partir dos relatórios “**Unacceptable: Responding to Technology-Facilitated Gender-Based Violence**”, da Women’s Legal Education and Action Front (LEAF) (2023), “**Technology-Facilitated Gender-Based Violence**”, de Suzie Dunn pelo Centre for International Governance Innovation (2020), e “**Glossary of Platform Law and Policy Terms**”, de Luca Belli, Nicolo Zingales e Yasmin Curzi (2021).



2.2 Glossário de TFGBV

Ação coordenada	Esforço organizado por múltiplos indivíduos em conjunto na Internet. Embora possa servir a propósitos positivos, pode envolver a propagação (orgânica ou artificial) de discursos de ódio, desinformação, spam ou ataque.
Ataque coordenado (ou ataque em massa)	Tipo de ação coordenada que envolve comportamentos maliciosos ou hostis em ambientes digitais. Caracteriza-se pela organização e execução de ações (orgânicas ou artificiais) para difamação, assédio ou ataques de negação de serviço (DDoS), com o objetivo de intimidar, silenciar ou prejudicar um indivíduo ou grupo. Ver também "mobbing" e "swarming".
Assédio virtual	Quando pessoas persistentemente buscam contato virtual com alguém que não deseja esse contato.
“Cheapfakes”/ “Shallow Fakes”	São a manipulação de conteúdos audiovisuais sem o uso de inteligência artificial (IA), a partir de montagens, alteração de plano de fundo ou cronologia para modificar a percepção do vídeo.
Deep Fakes	São imagens criadas ou alteradas por tecnologias de inteligência artificial (IA) que podem alterar também voz, imagens ao vivo, entre outros, para parecer que alguém fez, falou ou presenciou algo sem que a pessoa tenha de fato feito, dito, presenciado, etc..

<p>Denúncia Coordenada (“coordinated flagging”)</p>	<p>Uso das ferramentas de denúncia de uma plataforma digital com o objetivo de acionar os mecanismos de moderação de conteúdo para provocar a remoção ou a suspensão de um conteúdo.</p>
<p>Difamação</p>	<p>Embora a difamação não tenha surgido com as novas tecnologias, sendo tipificada pelo Código Penal brasileiro (art. 139), as maneiras de difamar alguém se tornam ampliadas por elas. Postagens, vídeos e fotos podem ser usadas fora de contexto ou contendo informações falsas para gerar difamação.</p>
<p>Discurso de ódio</p>	<p>O discurso de ódio é aquele que promove violência e perseguição contra pessoas integrantes de grupos sociopoliticamente minorizados. Inclui o ato de “espalhar, incitar, promover ou justificar” qualquer conteúdo relacionado ao “ódio racial, xenofobia, antissemitismo ou outras formas de ódio baseadas na intolerância, incluindo intolerância expressa pelo nacionalismo agressivo e etnocentrismo, discriminação e hostilidade em relação a minorias, migrantes e pessoas de origem imigrante” (Council of Europe, 1997).</p>
<p>Doxxing</p>	<p>Esse tipo de violência envolve a publicação não autorizada de dados sensíveis, como endereço residencial, número de telefone e outras informações pessoais, com o objetivo de causar danos à vítima. Por exemplo, uma mulher que sofre ameaças online pode ter seu endereço divulgado, o que potencialmente aumenta seu medo e ansiedade em relação à sua segurança pessoal (Curzi apud Citron, 2014, p. 58).</p>

<p>“Impersonation”/Falsa identidade</p>	<p>O termo em inglês “impersonation” se traduz como “personificação” e é usado para designar quando uma pessoa cria uma falsa identidade. Na legislação brasileira, os artigos 307 e 308 do Código Penal criminalizam o uso de identidades falsas.</p>
<p>Mobbing</p>	<p>Forma de ação coordenada em que um indivíduo é alvo de hostilidade persistente e repetitivo por parte de um grupo. Envolve ataques coordenados por múltiplos usuários contra uma pessoa, geralmente por meio de plataformas de mídia social, fóruns ou outros espaços digitais.</p>
<p>Trolling</p>	<p>O termo “troll” é usado para descrever o comportamento de alguém que posta mensagens deliberadamente provocativas ou desorientadoras, com a intenção de atrair as pessoas para uma resposta emocional ou para perturbar a discussão normal (p. 63, Curzi apud Phillips, 2015, p. 63).</p>
<p>“Sextortion”</p>	<p>Quando a extorsão é feita com ameaças do uso de imagens ou fotos de momentos íntimos obtidos com ou sem o consentimento da pessoa ameaçada.</p>
<p>Spyware/stalkerware</p>	<p>Quando alguém faz uso de aplicativos ou aparatos com a finalidade de monitorar alguém sem o seu consentimento. Muitas vezes atuam por meio de vírus e conseguem acesso à câmeras, localização e demais informações dos aparelhos eletrônicos de uso individual de alguém.</p>

<p>Swarming</p>	<p>Semelhante ao mobbing, é uma espécie de ataque online em que um grande número de usuários converge simultaneamente para atacar um alvo específico. É, em geral, um ataque de curta duração, mas com alta intensidade. Os perpetradores podem usar várias plataformas de forma simultânea para inundar a vítima de mensagens hostis, e até ataques cibernéticos, como hacking ou doxing (divulgação de informações pessoais). Visa sobrecarregar e desestabilizar psicologicamente a vítima.</p>
<p>Swatting</p>	<p>Nomeado assim em referência ao "Special Weapons and Tactics (SWAT)", o termo "swating" designa o ato de fazer falsas acusações à polícia a respeito de alguém para causar interrupção.</p>
<p>Shadowbanning</p>	<p>Shadowbanning significa a redução de visibilidade ou restrição de forma opaca a determinado perfil ou conteúdo. Assim, alguns conteúdos são "banidos" ou não distribuídos para o público sem que o seu produtor possa saber o real motivo.</p>
<p>Shadowpromotion</p>	<p>Em oposição ao "shadowbanning", o termo "shadowpromotion" é a promoção, também arbitrária, de determinados conteúdos nas redes, como desinformação e discurso de ódio. Ambas as práticas são problemáticas e sinalizam preferências "ocultas" dos sistemas de recomendação das plataformas.</p>

3. Censura na Internet

Um dos primeiros temas a serem tratados quando falamos de **violência online** é a **liberdade de expressão**, constantemente evocada para justificar discursos que, muitas vezes, infringem liberdades ao invés de garanti-las. Como nenhum direito fundamental é absoluto, o exercício da liberdade de expressão deve ser ponderado com outros direitos.

No âmbito normativo brasileiro, a liberdade de expressão emana da **dignidade da pessoa humana**, fundamento do Estado Democrático de Direito (**art. 1º, III**), e é tutelada pelo **art. 5º, inciso IX**, da **Constituição Federal de 1988**. É também um princípio ordenador do **Marco Civil da Internet (MCI)**, positivado em seu **art. 3º, inciso I**. Sua concretização e efetividade dependem do enfrentamento da censura e de limitações de expressões legítimas — i.e., aquelas que não violam outros direitos fundamentais. Além disso, a liberdade de expressão é garantida em diversos **tratados de direitos humanos** dos quais o Brasil é signatário, como a **Declaração Universal de Direitos Humanos (art. 19)** e a **Convenção Americana sobre Direitos Humanos (art. 13)**.

Nesta seção, procuramos explorar como o Estado regula o discurso online e como a censura privada pode ocorrer nos meios digitais. Além disso, apresentamos **quais são as ferramentas** presentes no ordenamento jurídico brasileiro para lidar com a liberdade de expressão de forma adequada.

3.1 Como o Estado regula a expressão online?

A regulação do discurso na Internet pelo Estado envolve uma complexa interação entre legislação e ações judiciais, as quais visam **equilibrar** a liberdade de expressão com a proteção de outros direitos fundamentais. Envolve o combate e a restrição ativa de discursos de ódio, desinformação e outras formas de comunicação potencialmente prejudiciais. Essa restrição pode ocorrer, no caso do Brasil, via **judicial**, como regra geral, ou **extrajudicial**, nas hipóteses definidas no MCI e por órgãos de defesa do consumidor. A diferença entre regulação legítima e censura reside na proporcionali-

dade e necessidade de medidas implementadas pelo Estado. Regulações legítimas devem interferir minimamente na liberdade de expressão e ser aplicadas apenas quando estritamente necessário para proteger outros direitos ou interesse público. Em contextos democráticos, **leis e regulamentos devem permitir o debate público e ser passíveis de revisão judicial** — evitando qualquer forma de restrição ilegítima do discurso.

Convenção Americana de Direitos Humanos — Artigo 13.

1. Toda pessoa tem direito à liberdade de pensamento e de expressão. Esse direito compreende a liberdade de buscar, receber e difundir informações e idéias de toda natureza, sem consideração de fronteiras, verbalmente ou por escrito, ou em forma impressa ou artística, ou por qualquer outro processo de sua escolha.
2. O exercício do direito previsto no inciso precedente **não pode estar sujeito a censura prévia**, mas a responsabilidades ulteriores, que devem ser expressamente fixadas pela lei e ser necessárias para assegurar:
 - a) o respeito aos direitos ou à reputação das demais pessoas; ou
 - b) a proteção da segurança nacional, da ordem pública, ou da saúde ou da moral públicas.

No âmbito digital, a proteção contra a censura não se limita à ação estatal de não remover conteúdo, mas se estende a uma obrigação de regulamentar outros atores. Devido à **eficácia horizontal dos direitos fundamentais**, que também incidem nas relações entre particulares, a norma também é aplicável a agentes privados. No Brasil, o **Marco Civil da Internet** é um exemplo de legislação que busca proteger a expressão online contra interferências arbitrárias de atores privados.

O **artigo 19 do MCI** estabelece a responsabilidade civil dos provedores de internet por conteúdos gerados por terceiros apenas após ordem judicial, visando proteger esses atores de serem indevidamente responsabilizados por conteúdos ilícitos de usuários. O dispositivo foi pensado a partir da compreensão do legislador de que a possível responsabilização desses atores por conteúdos de terceiros, poderia desencadear remoções em massa de qualquer conteúdo que pudesse ser compreendido como ilícito — incluindo aqueles legítimos e lícitos que poderiam estar em uma "zona cinzenta". Apesar desse mecanismo, não há uma legislação ou norma que proteja os usuários da remoção indevida por parte de provedores, moderadores de fóruns, administradores de plataformas ou outros usuários que possam buscar suprimir determinado conteúdo.

Casos de bloqueios indevidos de contas, remoção de conteúdo e alegação de redução de visibilidade — fenômeno categorizado como **shadowbanning** (v. página 26) — são recorrentes e usuários se queixam da falta de transparência e de mecanismos de devido processo por parte das plataformas para a contestação de tais medidas.

Desde 2020 tramita no Congresso Federal o **Projeto da Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet (PL 2.630/2020)**. O objetivo geral deste projeto de lei (PL) é trazer direitos aos usuários e deveres às plataformas. O texto faz ampla e expressa menção à liberdade de expressão. Na última versão do texto, apresentada em abril de 2023 pelo relator Deputado Orlando Silva (PCdoB), o **artigo 3º** define como alguns princípios norteadores:

III - o livre exercício da expressão e dos cultos religiosos, seja de forma presencial ou remota, e a exposição plena dos seus dogmas e livros sagrados;

IV – a liberdade de expressão, a liberdade de imprensa, o acesso à informação, o fomento à diversidade de informações no Brasil e a vedação à censura no ambiente online;

V – o livre desenvolvimento da personalidade, da dignidade, da honra e da imagem;

Além disso, o PL dedica uma seção inteira à "**Notificação pelo Usuário e Devido Processo nos Procedimentos de Moderação de Conteúdo**". Com isso, o projeto visa estabelecer regras e diretrizes para assegurar aos usuários **canais efetivos** para reclamação às plataformas quando forem vítimas de supressão indevida de seus discursos, i.e., direitos de **devido processo**.

Apesar de abordar temas mais amplos, o projeto de lei passou a ser popularmente conhecido como "**PL das Fake News**" — ou, ainda, como "**PL da Censura**" por atores políticos contrários ao combate à desinformação. Com isso, o PL foi associado pelo público à imposição de limitações às liberdades dos usuários, embora tal presunção seja equivocada.

Os dispositivos mencionados acima demonstram que o PL 2630/2020 pode ser um passo em direção ao combate à censura privada e falta de transparência nos meios digitais. Na realidade, o PL vincula os provedores a garantir em seus **Termos de Uso** mais **transparência** e **proteção à liberdade de expressão** aos usuários, bem como os obriga a adotar medidas para o **devido processo** nas decisões que afetam seus conteúdos e suas contas.

Enquanto o PL não está vigente, diversas formas de **indisponibilização de conteúdo e contas** e a **falta de mecanismos adequados** de devido processo e transparência nas plataformas digitais tornam a Internet um espaço menos seguro para minorias, causando danos bastante evidentes à liberdade de expressão e exercício de direitos civis e políticos desses grupos. No decorrer deste livro, exploramos alguns exemplos de como tais danos a direitos fundamentais se materializam, principalmente, para mulheres e pessoas LGBTQIA+ ativas politicamente.

3.2 Como a censura privada acontece nas redes sociais?

A regulação do discurso e conteúdo que circulam nas redes sociais ocorre principalmente a partir de medidas implementadas pelas próprias plataformas. De forma legítima, as plataformas estabelecem e aplicam suas políticas de conteúdo e termos de serviços, que definem o que é ou não permitido. Isso inclui a remoção ou restrição de conteúdos que são considerados inapropriados, como discurso de ódio, desinformação ou material com conteúdo sexual explícito.

Não obstante, os mecanismos de moderação de conteúdo podem ser falhos e as práticas das plataformas pouco transparentes, produzindo questionamentos sobre a legitimidade (HAGGART; KELLER, 2021) de tais ações, sobre – tudo quando o conteúdo restringido é lícito e não viola tais políticas.

A censura privada pode ser ocasionada por ingerência das próprias plataformas, conforme mencionado acima, ou por intervenções externas de terceiros. É possível que a censura seja materializada, por exemplo, por meio de:

- **Redução de visibilidade** de forma oculta, prática também conhecida como "**shadowbanning**";
- **Denúncia coordenada** em massa por parte de grupos de pessoas ou a partir de automatização;
- Prática de **spam**, a partir da postagem de conteúdos em massa que geram incômodo e inviabilizam a comunicação;
- **Ataques coordenados** a perfis específicos (ou *dogpilling*);
- **Hackeamento** de contas ativas, inviabilizando um canal de contato utilizado por defensores de direitos humanos;
- **Autocensura**, induzida por receio de hostilidades ou reações.



Shadowbanning

A censura por meio de “**shadowbanning**” ocorre quando as próprias redes reduzem o alcance de determinados usuários, sem transparência alguma sobre como a decisão foi tomada. Muitas vezes, o usuário sequer sabe o real motivo da diminuição do engajamento e/ou banimento de um post.

A prática de shadowbanning foi endereçada pela **Lei de Serviços Digitais Europeia** (Digital Services Act — DSA), em seus **artigos 14 e 17**, que exigem que os usuários sejam informados quando sofrerem alguma redução de visibilidade de seus conteúdos.

Lei de Serviços Digitais Europeia

Artigo 14: "Os prestadores de serviços intermediários **devem incluir nos seus termos e condições** informações sobre **quaisquer restrições** que imponham em relação à utilização do seu serviço no que diz respeito às informações fornecidas pelos destinatários do serviço. Essas informações devem incluir dados sobre **quaisquer políticas, procedimentos, medidas e ferramentas utilizadas para efeitos de moderação de conteúdos**, incluindo a tomada de decisões algorítmicas e a análise humana, bem como as regras processuais do seu sistema interno de tratamento de reclamações. Deve ser apresentado numa linguagem clara, simples, inteligível, de fácil utilização e inequívoca, e deve estar disponível ao público num formato facilmente acessível e legível por máquina."

Art. 17 da DSA: 1. Os prestadores de serviços intermediários **devem fornecer uma exposição clara e específica dos motivos a quaisquer destinatários afetados por qualquer uma das seguintes restrições impostas** com o fundamento de que as informações fornecidas pelo destinatário do serviço são conteúdos ilegais ou incompatíveis com os seus termos e condições: (a) **quaisquer restrições à visibilidade de conteúdos produzidos pelo destinatário do serviço**, incluindo a remoção de conteúdos, a desativação do acesso a conteúdos ou a despromoção de conteúdos;

Denúncia coordenada

Conforme relatório publicado pela Coding Rights e InternetLab (2017), a censura é uma das principais formas de violência contra a mulher e minorias sociais nos meios digitais. Além do *shadowbanning*, outra forma de materialização da censura, que afeta significativamente mulheres e ativistas, é a **denúncia coordenada** de conteúdos publicados por elas (Belli, Zingales, Curzi, 2021, p. 79).

Tal forma de violência é especialmente problemática na Internet não apenas pela facilidade do ato de denunciar e do caráter anônimo dessas denúncias, mas, principalmente, pela falta de mecanismos eficientes para contestar a decisão a respeito da retirada ou não da postagem e/ou indisponibilidade da conta.

O uso de determinados termos considerados violentos em determinados contextos, como “sapatão”, “preta” e “gay”, são recorrentemente utilizados dentro das comunidades de maneira ressignificada. Temos assim, por exemplo, "Marcha das Vadias" e "Visibilidade Sapatão". Neste cenário, no entanto, a moderação de conteúdo das plataformas costuma ser acionada por grupos maliciosos que **denunciam, de forma coordenada, conteúdos de ativistas.**

Além disso, o próprio algoritmo das redes sociais reduz o alcance dos conteúdos associados aos termos porque os considera, de forma automática, como violadores de suas políticas de comunidade ou termos de uso. Esse processo ocorre, principalmente, devido à falta de contexto e diversidade nas bases de dados que alimentam a moderação automatizada de conteúdo dessas plataformas.

Caso 1: A Censura à Lola Aronovich

O blog feminista "Escreva Lola Escreva", gerenciado pela ativista e professora da Universidade Federal do Ceará, **Lola Aronovich**, foi alvo de censura após ser atacado por grupos de ódio na Internet. As denúncias em massa levaram o Google a censurar várias publicações do blog e retirar seu blog do ar.



Há anos, Lola enfrenta agressões e ameaças de masculinistas. Um dos principais *chans* desses grupos, o Dogolachan, — alvo de diversas investigações da Polícia Federal, como a Operação "Underground" — enviou um e-mail ao reitor da universidade com ameaças de atentado caso ela não fosse demitida. Com a denúncia coordenada, o Google retirou o blog de Lola do ar.

O que são *chans*?

Chans, abreviação de channels (canais em inglês) são fóruns descentralizados com anonimato permitido, em que “grande parte de seus participantes tendem a se opor à mercantilização e à percepção de domesticação, feminização e integração da cultura da Internet” (Nagle, 2017).

Após a intervenção do Google, houve uma mobilização em apoio à Lola. A partir da hashtag "#GoolgePareDeCensurarALola" no antigo Twitter, usuários questionaram a ação da empresa, considerando-a um ataque à liberdade de expressão. Lola explicou que a justificativa dada pelo Google para a remoção foi a presença de uma imagem de abuso sexual infantil no blog. No entanto, após a revisão da decisão, ficou constatado que a imagem era um conteúdo de denúncia. Apesar da restauração de seu blog, o incidente reflete os desafios enfrentados por ativistas feministas — frequentemente alvos de **censura privada por moderação inadequada** de conteúdos de denúncia à violências.



Caso 2. O Hackeamento de Janja da Silva



A atual primeira dama do Brasil, Janja da Silva, é uma figura politicamente ativa, amplamente reconhecida pelo seu trabalho de promoção à assistência para as populações historicamente minorizadas.

Janja se tornou um alvo preferencial para ataques coordenados desde a campanha presidencial, como mapeado pelo MonitorA, projeto fruto de parceria entre InternetLab, Revista Azmina e Núcleo Jornalismo (2022). No dia 11 de dezembro de 2023, o perfil da primeira-dama na rede social “X” foi hackeado e utilizado para a publicação de ofensas e xingamentos carregados de misoginia.

*"Minha conta do X foi hackeada e, por **minutos intermináveis**, foram publicadas mensagens **misóginas** e **violentas** contra mim. Posts **machistas** e **criminosos**, típicos de quem despreza as mulheres, a convivência em sociedade, a **democracia** e a **lei**".*

FONTE: Terra Notícias. 12/12/2023. <https://bitly.ws/36QCC>

O papel das plataformas na segurança de seus usuários

O caso de Janja evidencia o quanto é vital que as plataformas estabeleçam canais de comunicação diretos e eficientes com seus usuários, principalmente personalidades públicas relevantes e autoridades governamentais, devido aos riscos para a segurança nacional.

A **transparência** também possui um papel crucial: as plataformas devem ser **claras** e **coerentes** quanto às suas políticas de segurança e aos procedimentos adotados em casos de ataques, garantindo que usuários possam compreender as medidas de proteção disponíveis e como podem ser utilizadas.

Plataformas como o "X" podem gerar receita significativa a partir de interações e engajamento de conteúdos controversos ou sensacionalistas, incluindo aqueles decorrentes de ataques cibernéticos a figuras públicas. Esse **modelo de negócios** pode criar um ciclo vicioso onde o comportamento nocivo é não apenas tolerado, mas indiretamente incentivado. Portanto, é essencial que essas plataformas revisitem seus modelos de monetização, assegurando que não estejam contribuindo para a proliferação de ataques digitais ou desinformação.

3.3 Como posso recorrer de censura privada?

Apesar de a censura ser expressamente vedada no ordenamento jurídico brasileiro, bem como por tratados internacionais de direitos humanos, tais disposições não acompanharam as evoluções tecnológicas. Assim, as diversas formas pelas quais a censura pode ocorrer nos meios digitais, e que acentuam a vulnerabilidade de determinados grupos a ataques maliciosos, exige uma atuação mais proativa das empresas na proteção e defesa de direitos humanos no ambiente digital.

Ainda que limitados e com um procedimento pouco transparente, algumas plataformas contam com mecanismos internos de apelação sobre suas decisões de restrição de conteúdos e/ou contas. Tal mecanismo existe na maioria das grandes plataformas, como o Facebook, Instagram, Twitter e Google. O Facebook, por exemplo, conta com o **Oversight Board**, uma entidade que mais se aproxima de um órgão julgador independente e decide sobre eventuais apelos em relação a um conteúdo removido.

Esses mecanismos internos evitam que usuários tenham que optar por uma via morosa, custosa e inconstante, como a via judicial, para contestar as decisões das plataformas. Geralmente, a atuação judicial para tais casos é pautada em regras gerais do **Código Civil** ou do **Código do Consumidor**, seja para a manutenção do conteúdo no ar, ou para a indenização por eventuais danos sofridos pela remoção equivocada do conteúdo.

Embora a análise feita pelo Poder Judiciário deva considerar as circunstâncias individuais do caso, o êxito na via judicial pode ser dificultado pela ausência de dispositivos legais relacionados à matéria específica. Não há legislação no Brasil que estabeleça para as plataformas uma obrigação relacionada à implementação de mecanismos mais céleres de resolução de controvérsias no ambiente digital. As respostas atuais ainda são insatisfatórias, sendo necessário que avancemos em medidas adequadas contra a censura privada e ataques online. Neste cenário, a Internet segue sendo um espaço hostil às minorias, com destaque para mulheres, grupo mais afetado pela falta de regulação das redes sociais no país.

Segundo o relatório “Violência de gênero facilitada pela tecnologia na era da IA generativa: Tendências globais e recomendações da UNESCO”, a violência de gênero online, mais especificamente destinada à mulheres e meninas, é um fenômeno global. A maior parte dos estudos realizados sobre o tema indicam que mulheres jornalistas e políticas são particularmente vulneráveis a esses ataques.

Uma estimativa realizada pela Plan International (2020), por exemplo, com 14 mil meninas e mulheres de 22 países apontou que 58% delas já foram vítimas de alguma forma de violência online. De acordo com a ONU Mulheres (2021), no mundo árabe 60% das mulheres sofreram violência online. Pesquisa da UNESCO (2019) com 901 jornalistas apontou que 73% delas já foram vítimas de violência no ambiente online. Com relação às mulheres que exercem cargos políticos, segundo estudo da Union Interparlementaire (2021), na África, 46% das parlamentares já foram alvo de ataques sexistas online. Um levantamento similar na Europa indicou que esses ataques já vitimaram 58% das mulheres parlamentares.

4. Crimes de ódio online

Crimes de ódio online se referem à publicação de conteúdos ou ações que podem afetar a dignidade humana de indivíduos e grupos com base em suas identidades. Esses crimes podem assumir várias formas e são amplificados pela natureza transnacional e muitas vezes anônima da Internet. No Brasil, os crimes de ódio online podem ser enquadrados em diversos tipos penais, dependendo da natureza específica da conduta. Alguns destes são:

Racismo (Lei nº 7.716/1989)	Trata-se de crime inafiançável e imprescritível no Brasil e as penas variam conforme a natureza específica do ato discriminatório tipificado em lei.
Injúria racial (Artigo 140, § 3º do Código Penal)	Ocorre quando ofensas racistas são direcionadas a uma pessoa específica. Com a edição da Lei nº 14.532/2023, a conduta é equiparável ao racismo e a pena passou a ser de reclusão de 2 a 5 anos e multa.
Homotransfobia (STF, Mandado de Injunção 4733, em 2019 e 2023)	Postagens de teor homofóbico ou transfóbico são passíveis de punição. Em 2019, no julgamento do MI 4733, o STF equiparou a homofobia e a transfobia ao crime de racismo. Em 2023, julgando um recurso sobre esse mesmo MI, reconheceu que atos ofensivos praticados contra pessoas da comunidade LGBTQIAPN+ podem ser enquadrados como injúria racial.
Lei nº 13.642/2018 (Lei Lola)	A Lei nº 13.642/2018, apelidada "Lei Lola", em homenagem à ativista Lola Aronovich, acrescentou como competência da Polícia Federal a investigação de "VII – quaisquer crimes praticados por meio da rede mundial de computadores que difundam conteúdo <u>misógino</u>, definidos como aqueles que propagam o ódio ou a aversão às mulheres". É a primeira vez que aparece uma definição de "misoginia" na legislação brasileira.

<p>Disseminação de Imagens ou Informações Pessoais (Lei nº 12.737/2012 - Lei Carolina Dieckmann)</p>	<p>A disseminação de imagens ou de informações pessoais é punida pelo art. 154-A do Código Penal, incluído pela Lei Carolina Dieckman. O artigo prevê a punição para a "invasão de dispositivo informático alheio, com o fim de obter, adulterar ou destruir dados ou informações sem autorização ou instalar vulnerabilidades para obter vantagem ilícita". A pena mínima é de detenção, de 3 meses a 1 ano, e multa, mas pode ser maior e mais grave a depender das circunstâncias do caso.</p>
<p>Stalking/Perseguição (Lei nº 14.132/2021)</p>	<p>Ocorre quando alguém pratica atos <u>reiterados</u> de perseguição que ameaçam a integridade psicofísica de uma pessoa, podendo limitar sua capacidade de locomoção, invadir, ou perturbar sua vida privada e autonomia. O tipo penal inclui também ações praticadas por meios digitais (<i>cyberstalking</i>), como envio de mensagens, e-mails e publicações que possam constituir prática reiterada de perseguição e assédio. A pena mínima para o crime é de reclusão, de seis meses a dois anos, e multa, podendo ser majorada ou agravada em situações específicas.</p>
<p>Incitação/Apologia ao crime ou ao criminoso (Artigos 286 e 287 do Código Penal)</p>	<p>Fazer publicamente apologia de um crime ou de um criminoso. A pena é de detenção, de três a seis meses, ou multa.</p>
<p>Difamação (Artigo 139 do Código Penal)</p>	<p>Imputar a alguém um fato ofensivo à sua reputação. A pena é de detenção, de três meses a um ano, e multa.</p>
<p>Calúnia (Artigo 138 do Código Penal)</p>	<p>Imputar falsamente a alguém um fato definido como crime. A pena é de detenção, de seis meses a dois anos, e multa.</p>

4.1 Contexto legislativo sobre crimes de ódio no Brasil

Em janeiro de 2023, a **Lei nº 14.532**, sancionada pelo Presidente Lula, designou mudanças significativas na Lei Caó (Lei nº 7.716/1989). Com a edição, a **injúria racial foi equiparada ao crime de racismo** e tipificada no art. 2º -A da Lei Caó. De tal forma, essa modalidade de injúria passa a ter o mesmo tratamento jurídico do crime de racismo: **imprescritibilidade, inafiançabilidade e incondicionalidade da ação penal pública**.

Com relação à **homotransfobia**, uma decisão do Supremo Tribunal Federal no Mandado de Injunção 4733, em 2019, já havia equiparado esse tipo de conduta ao crime de racismo. Todavia, embargos de declaração contra o acórdão foram apresentados pela Associação Brasileira de Lésbicas, Gays, Bissexuais, Travestis, Transexuais e Intersexos (ABGLT). De acordo com a ABGLT, a decisão estava sendo interpretada de forma equivocada, no sentido de que a ofensa contra grupos LGBTQIAPN+ configura racismo, mas a ofensa à honra de pessoas pertencentes a esses grupos vulneráveis não configura o crime de injúria racial. Em 2023, o Plenário do STF julgou os embargos procedentes e reconheceu que o entendimento também se aplica ao crime de injúria racial.

Sobre a **misoginia**, este conceito foi definido pela primeira vez na legislação brasileira a partir da **Lei Lola** (em homenagem à ativista Lola Aronovich). A norma atribuiu competência à Polícia Federal para a investigação de crimes virtuais contra mulheres “que difundam **conteúdo misógeno**, definidos como aqueles que propagam o ódio ou a aversão às mulheres”. De tal forma, conteúdos misóginos também são passíveis de punição legal.

Caso 3. Ataques à Érika Hilton

A deputada federal Erika Hilton assumiu o cargo em janeiro de 2023 pelo estado de São Paulo e é a primeira mulher negra e trans a ocupar uma cadeira na Câmara. Hilton tem sido alvo de ataques nas redes, que vão desde xingamentos racistas, misóginos e transfóbicos até ameaças à integridade física e à vida da deputada.



Mulheres em cargos políticos e/ou na posição de figuras públicas, de maneira geral, tendem a ser os principais alvos de grupos mobilizados para impulsionar discurso de ódio na Internet (LAMENSCH, 2021). Além de Érika Hilton, outros casos ganharam destaque no Brasil nos últimos anos, como a desinformação sobre o feminicídio político de Marielle Franco, enquanto exercia o cargo de vereadora do Rio de Janeiro, e os ataques à Patrícia Campos Mello, jornalista expatriada após sofrer inúmeras ameaças virtuais e presenciais.

Situações como essas aumentam a sensação de insegurança das mulheres que ocupam cargos políticos ou publicamente relevantes no país. Tratando-se de uma mulher negra e trans, as violências contra Érika são ainda mais graves. Além da hostilização rotineira, que visa diminuir a representatividade política de mulheres, existe ainda a articulação de outros estereótipos — de animalização e agressividade.

4.2 Como recorrer quando sofro crimes de ódio nas redes?

Abaixo, listamos algumas das principais orientações e recursos para vítimas de crimes de ódio na Internet.

1. **Documente as ofensas:** Capture evidências dos conteúdos ofensivos (*screenshots*, links, etc.).
2. **Denuncie nas próprias plataformas:** Utilize as ferramentas internas das redes para reportar o conteúdo ofensivo.
3. **Registre um boletim de ocorrência:** É possível levar o caso a uma delegacia e registrar um boletim de ocorrência. Procure uma Delegacia especial, como a Delegacia de Crimes Raciais e Delitos de Intolerância (DECRADI) ou a Delegacia de Atendimento à Mulher (DEAM), para casos de homotransfobia e racismo ou misoginia, respectivamente. Além disso, é possível registrar ocorrências online por meio de delegacias virtuais.
4. **Busque assessoria especializada:** Considere consultar um advogado ou a Defensoria Pública para avaliar a possibilidade de ajuizar uma ação. A organização **Safernet** também possui um *helpline* para ajuda ou orientação sobre crimes virtuais e um *hotline* para denúncia anônima (<https://new.safernet.org.br/content/crimes-na-web>).
5. **Denuncie à Polícia Federal online:** O "Comunica PF" é o canal que permite a comunicação online de crimes de atribuição investigativa da Polícia Federal, conforme estabelecido pelo § 1º do art. 144 e art. 109 da Constituição Federal, pela Lei nº 10.446/2022 e de acordo com o § 3º do art. 5º do Código de Processo Penal-CPP.

A partir do arcabouço legal mencionado, as autoridades policiais têm a responsabilidade de investigar e monitorar os responsáveis pelos ataques, respeitando sempre as balizas legais estabelecidas. Isso inclui a observância de direitos constitucionais como o **direito à privacidade** e o **sigilo das comunicações**, conforme delineado na Constituição Federal e nas leis específicas como o Marco Civil da Internet (Lei nº 12.965/2014).

Tecnicamente, as forças policiais utilizam uma gama de ferramentas avançadas para rastrear a origem dos ataques cibernéticos. Estas ferramentas podem incluir o uso de *software* de rastreamento de IP, análise de dados de tráfego na Internet e tecnologias de monitoramento de comunicações online. Em conformidade com a legislação, como o MCI (**arts. 10 a 17**), a polícia pode requerer às plataformas digitais os registros de conexão e de acesso a aplicações, que são fundamentais para identificar os autores dos crimes.

O MCI prevê que as plataformas de mídia social colaborem com as investigações, fornecendo informações apenas quando solicitado pelas autoridades judiciais ou administrativas. Essa colaboração é regulamentada de forma a equilibrar a necessidade de investigação com a proteção dos direitos dos usuários das plataformas.

As autoridades policiais podem colaborar com a Agência Brasileira de Inteligência Nacional (ABIN) e com agências internacionais para investigar crimes que ultrapassam fronteiras nacionais. Essas ações estão alinhadas com tratados internacionais e acordos de cooperação em matéria de segurança cibernética e combate ao crime online, como a **Convenção de Budapeste**, promulgada no Brasil em abril de 2023.

4.3 Qualquer um pode ser vítima de discurso de ódio?

Embora qualquer pessoa possa sofrer xingamentos, *bullying*, ameaças ou outros tipos de agressões, o **discurso de ódio** não vitima qualquer pessoa. Ele **é aquele que atinge, especificamente, pessoas cuja identidade pode ser acionada de maneira a evocar opressões sistematicamente existentes, fazendo com que a marginalização sofrida seja agravada pelas possibilidades criadas pela internet.** Segundo dados de 2021 do Observatório Brasileiro de Violência Online, da Universidade de Brasília, as mulheres são as principais vítimas de discurso de ódio online no contexto brasileiro.

O discurso de ódio utiliza determinados marcadores sociais que podem fazer parte da identidade de pessoas, em geral sub-representadas no poder político e em demais esferas de poder da sociedade, no âmbito público ou privado. É uma prática que pode ser observada nos diversos espaços onde as **assimetrias de poder** se fazem evidentes, especialmente quando há disputa de poder e/ou representação política.

Cyberbullying e discurso de ódio

Frequentemente, a prática de *bullying* ou *cyberbullying* é associada a discurso de ódio – até mesmo estando na mesma categoria de violação nas políticas de comunidade de algumas das principais plataformas de redes sociais. Em dezembro de 2023 foi aprovado no Senado o PL 4.224/21, que inclui no Código Penal a modalidade virtual de intimidação sistemática – **cyberbullying**. A norma prevê uma punição maior quando o crime é praticado contra crianças.

Com o avanço da Internet, as redes sociais se tornam um campo facilitação para que também esse tipo de discurso ocorra. Caso você presencie ou seja vítima de algum tipo de violência nas redes sociais, procure acionar os **mecanismos de denúncia**, tanto nas plataformas quanto externos, a fim de buscar o fim da propagação do discurso de ódio e outras formas de violência nas redes.



5. Ameaças à integridade psicofísica

Crimes virtuais são rotineiramente subestimados na sociedade. Muitas vezes, as vítimas são confrontadas com sugestões simplistas como "*é só sair de tal site*" ou "*é só fechar o computador*", o que ignora a gravidade e o impacto real desses crimes. Tal pensamento falha em reconhecer que a violência online pode ter consequências tangíveis e muito sérias e no mundo físico.

Eles podem, por exemplo, afetar significativamente a saúde mental das vítimas: como mencionado por Curzi (2023), mulheres afetadas por ameaças ou assédio online podem sofrer de **ansiedade e depressão severa**, a ponto de deixarem de participar de forma pública nas redes. Tais impactos são um claro indicativo de que ações no ambiente virtual podem causar danos reais e duradouros, estendendo-se muito além do espaço digital e afetando a concretização de direitos fundamentais, como a **liberdade de expressão**.

Segundo o "Relatório do Observatório das Condenações Judiciais em 2ª Instância até o ano de 2022" (2023) feito em parceria pela Faculdade Baiana de Direito, o PNUD e JusBrasil, **60% de todas as denúncias de violência na Internet são feitas por mulheres**, principalmente **mulheres negras**.

O relatório da UNESCO "La violence de genre facilitée par la technologie à l'ère de l'intelligence artificielle générative" (2023) menciona que **jornalistas negras, indígenas e judias** relatam taxas mais altas de violência online do que suas colegas brancas. As variações também se manifestam de acordo com a orientação sexual, **com 72% das mulheres heterossexuais sendo alvo, contra 88% de mulheres lésbicas e 85% de mulheres bissexuais**.

Além disso, a ameaça de violência física na Internet possui características particulares e pode ser mais pronunciada devido a elementos interseccionais como origem étnica, idade, orientação sexual, religião, identidade de gênero, status socioeconômico, casta, deficiência e status de refugiado. Não apenas, mas frequentemente, esses crimes têm como foco grupos minoritários e mulheres, sobretudo mulheres pretas e pardas, perpetuando e intensificando desigualdades e preconceitos já existentes na sociedade.

Casos emblemáticos ilustram como pessoas que conquistaram posições de poder, ainda dominadas por homens brancos cisgênero das classes mais altas, enfrentam desafios significativos. Essas pessoas, ao exercerem seus direitos políticos de forma mais ativa e visível, frequentemente se tornam alvos de ataques e ameaças sistemáticas. Essas ações visam, em muitos casos, minar sua permanência e eficácia em espaços de poder e de tomada de decisão.

Além de Erika Hilton (PSOL), a deputada Talíria Petrone (PSOL) tem enfrentado injúrias raciais e ameaças de morte ao longo de sua carreira. Outros exemplos incluem as deputadas estaduais Lohanna França (PV), Bella Gonçalves (PSOL), Andreia de Jesus (PT) e Beatriz Cerqueira (PT), e vereadoras Iza Lourença (PSOL) e Cida Falabella (PSOL), que sofreram ameaças de morte e "estupro corretivo" em 2023. Tais ameaças são empregadas como método de intimidação, caracterizando uma modalidade difusa de violência política de gênero. Essas condutas já são tipificadas no art. 147 do Código Penal, que trata das ameaças, na Lei Maria da Penha, sobre violência contra mulher e, recentemente, como crimes de homotransfobia e racismo, como exposto acima.

No entanto, no ambiente virtual há espaço para novas táticas e condutas que podem não ser tão bem compreendidas pelas autoridades ou pelas plataformas. Pense, por exemplo, em um perfil anônimo que poste apenas o nome da Escola onde o filho de uma pessoa relevante estuda. Dificilmente a postagem será objeto da moderação de conteúdo. Pense também na possibilidade de um perfil no LinkedIn visualizar todos os dias o perfil de outra pessoa. Dificilmente as polícias compreenderão tal conduta como ameaçadora. Essas situações ressaltam a necessidade de atualizações e adaptações na legislação brasileira para abordar de forma mais eficaz as ameaças no meio digital. Para o segundo caso, tivemos a edição da **Lei de Stalking**.

5.1 A Lei de Stalking

O artigo 147-A, inserido no Código Penal pela Lei 14.132/21, institui o crime de perseguição, ou *stalking*, caracterizado por condutas que constroem uma pessoa de maneira acentuada, invadindo sua privacidade e obstruindo o exercício de liberdades básicas.

Stalking é um termo da língua inglesa cuja tradução direta seria “perseguição”. A pessoa que persegue, seja online ou presencialmente, é chamada de **stalker**. Quando a conduta ocorre online, ela é chamada de **cyberstalking**.

O crime de *stalking* inclui a perseguição persistente e indesejada por meio físico e/ou digital, como em redes sociais e aplicativos de mensagens. É uma forma de violência que pode ter sérios impactos na vida das vítimas, afetando sua saúde mental e bem-estar físico. No meio virtual, a perseguição pode ocorrer, por exemplo, pelo envio de mensagens, recados, convites, solicitações para seguir, ofensas recorrentes divulgadas nas redes sociais ou, ainda, visualização recorrente de um perfil que pode representar ameaça à vítima.

Segundo dados do Fórum Brasileiro de Segurança Pública (FBSP), em 2022, o Brasil registrou um aumento significativo nos casos de stalking, com mais de 56 mil denúncias ao longo do ano, representando um aumento de 75% em relação ao ano anterior. São Paulo foi o estado com o maior número de casos, totalizando mais de 17 mil ocorrências. Outros estados com altas taxas de incidência incluem Rio Grande do Sul, Paraná, Santa Catarina e Minas Gerais. Esse aumento nas denúncias pode estar ligado a uma maior conscientização sobre o crime de perseguição e à disposição das vítimas em denunciar tais incidentes. A pandemia de Covid-19 também pode ter produzido impacto no aumento dos casos de perseguição online, ou cyberstalking.

Crime de Stalking

Art. 147-A, CP. Perseguir alguém, reiteradamente e por qualquer meio, ameaçando-lhe a integridade física ou psicológica, restringindo-lhe a capacidade de locomoção ou, de qualquer forma, invadindo ou perturbando sua esfera de liberdade ou privacidade. Pena – reclusão, de 6 (seis) meses a 2 (dois) anos, e multa.

O crescimento acentuado, no entanto, ainda pode estar subestimado devido à subnotificação. Um dos desafios na quantificação exata desses casos é a falta de um sistema de catalogação uniforme em todo o Brasil. Por exemplo, em contraste com as mais de 17 mil ocorrências de São Paulo, o Rio de Janeiro apresentou um número muito menor de casos, o que levanta questões sobre a precisão e a

abrangência da coleta de dados. A discrepância pode ser parcialmente explicada pela maneira como os estados registram esses crimes, especialmente no que diz respeito à sua manifestação no meio digital. Outro fator importante para a subnotificação é a recente criminalização da perseguição online no Brasil e uma possível falta de conhecimento sobre a legislação pela população em geral e por autoridades.

Antes de abril de 2021, quando a perseguição online foi oficialmente reconhecida como crime, muitos casos eram enquadrados apenas como contravenção penal. Isso significa que muitos estados ainda podem não ter sistemas adequados para registrar e monitorar casos de *stalking*, especialmente aqueles que ocorrem com uso de instrumentos tecnológicos.

5.2 Como agir quando acredito que estou sendo vítima de *stalking* ou ameaça?

Para denunciar o crime de *stalking*, diversos elementos podem ser usados como prova, entre eles: capturas de tela, fotos, áudios, gravações de áudio e vídeo como câmeras de segurança, registro de entrada em edifícios, histórico de ligações ou testemunhas que possam comprovar o ocorrido, por exemplo. Para manter a veracidade do que for apresentado, é recomendado que a vítima se dirija a um cartório para que uma pessoa de fé pública possa atestar o material reunido.

Recomendações para vítimas:

- **Registre as provas:** Documente todas as provas das ações do stalker ou da pessoa que ameaça, salvando a URL (link) das postagens, mensagens, e-mails, *screenshots* (captura de tela) de redes sociais, entre outros. Essas evidências são essenciais para um eventual processo legal.
- **Bloqueie o contato:** Se o stalker ou pessoa que a ameaça for conhecido, cabe bloquear o contato das redes sociais para evitar a contínua vigilância e denunciar o caso nos canais eventualmente disponíveis da própria plataforma.

- **Registre um boletim de ocorrência:** A denúncia pode ser feita nas Delegacias de Crimes Cibernéticos, Delegacias Comuns ou Especializadas (como a DEAM). Ainda que o stalker ou a pessoa que ameaça seja desconhecida, é possível registrar o boletim de ocorrência. A polícia possui meios de investigar e identificar o autor utilizando procedimentos e técnicas específicos para crimes cometidos no ambiente virtual.
- **Assistência jurídica:** A vítima poderá acionar a justiça para que esta determine que os provedores de aplicação e de conexão informem os dados de acesso vinculados à conexão e perfil do criminoso, como números de IP, horários de login, nome e endereço associados ao usuário etc. Conforme disposto no MCI, os provedores de conexão e de aplicação devem manter os registros guardados pelos prazos de 1 ano e de 6 meses, respectivamente. Contudo, mediante determinação judicial, esse prazo pode ser estendido a fim de viabilizar e garantir a investigação dos crimes praticados virtualmente.
- **Acione as medidas legais:** Com as informações em mãos, a vítima pode iniciar um processo contra o *stalker* ou a pessoa que a ameaça, seja na esfera cível ou criminal.

6. Privacidade, honra e imagem na Era Digital

À medida que grandes empresas de tecnologia enfrentam escândalos relacionados à coleta indevida de dados, como a coleta de dados de usuários do Facebook para marketing político direcionado envolvendo a empresa **Cambridge Analytica** em 2017, a preocupação com a privacidade online torna-se uma questão cada vez mais premente. O temor com relação à vigilância constante pelas plataformas digitais é agravado pela alta conectividade inerente à transformação digital que interliga até mesmo atividades diárias básicas ao uso da internet. O conceito de "Internet das Coisas" exemplifica bem essa realidade. Agora, não são apenas os celulares que estão conectados e suscetíveis à coleta de dados. *Gadgets* como relógios inteligentes, óculos VR e eletrodomésticos modernos são utilizados para coletar e monitorar informações pessoais. Considere, por exemplo, um refrigerador inteligente que rastreia seus hábitos alimentares ou, ainda, um assistente de voz que grava as suas conversas.

Além disso, a inteligência artificial (IA) traz novos desafios para o debate sobre a privacidade. O reconhecimento facial em fotos e vídeos compartilhados nas redes sociais pode ser usado para coletar dados biométricos sem o consentimento explícito do usuário. Enquanto expressão da dignidade humana, é dever do Estado empreender o máximo esforço possível para impedir ou cessar as violações à privacidade — direito tutelado pela **CRFB/1988 em seu artigo 5º, X, e pelo Código Civil, em seu artigo 21.**

Art. 21, CC. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.

A Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados (LGPD), foi responsável por estabelecer que o tratamento de dados pessoais deve estar fundamentado em bases legais claras, respeitando princípios essenciais delineados em seu **artigo 6º**. Entre esses princípios, destacam-se a **finalidade**, a **adequação** e a **necessidade**.

O princípio da **finalidade** exige que a coleta de dados tenha uma razão legítima, específica e explícita, assegurando que o tratamento dos dados seja compatível com os objetivos declarados. A **adequação**, por sua vez, garante que os dados coletados sejam pertinentes e não excedam o necessário para atingir esses objetivos. Por fim, o princípio da **necessidade** impõe limites ao tratamento de dados, restringindo-o ao mínimo necessário para cumprir com as finalidades estabelecidas.

A LGPD também previu a criação de uma autoridade dedicada à fiscalização da adequação de entidades privadas e públicas à Legislação, a Autoridade Nacional de Proteção de Dados (ANPD). Em 2022, a ANPD, em parceria com o Tribunal Superior Eleitoral (TSE), publicou um "**Guia de Eleições**", responsável por trazer orientações práticas sobre a aplicação da LGPD nas eleições, explicar aspectos obrigatórios da lei no contexto eleitoral e recomendar boas práticas a serem seguidas pelos candidatos, partidos políticos e coligações. O Guia pode ser acessado em: https://www.gov.br/anpd/pt-br/assuntos/noticias/guia_lgpd_final.pdf.

Embora a LGPD não trate especificamente de violência política, seus princípios e disposições sobre o tratamento de dados pessoais oferecem ferramentas valiosas para salvaguardar a privacidade e a segurança de informações pessoais a fim de que não sejam utilizadas indevidamente no contexto da violência política.

6.1 Quais são meus direitos quanto à minha imagem e honra?

Os direitos à **imagem** e à **honra** são amplamente protegidos no Brasil, conforme estabelecido pelo **artigo 5º, incisos V e X**, da Constituição Federal de 1988. Esse artigo enquadra os direitos à imagem e à honra como direitos fundamentais, cruciais para garantir a **dignidade** e a **integridade** do indivíduo na sociedade. O **artigo 20 do Código Civil** reforça expressamente a proteção da imagem, proibindo, via de regra, o seu uso ou exposição não autorizada e estabelecendo a possibilidade de indenização caso atinja a honra da vítima, por exemplo.

Ponderando o **direito à imagem** com a **liberdade de expressão**, há **exceções** a essa regra geral. Uma delas, por exemplo, é a autorização do uso da imagem quando necessária para a manutenção da ordem pública ou para fins **jornalísticos**, sem intuito de ofensa ou exposição indevida. As exceções, contudo, devem ser interpretadas de forma restritiva para evitar abusos.

Para coibir o abuso da liberdade de expressão no contexto da honra e da imagem, o Código Penal brasileiro, nos artigos 138 a 140, aborda os crimes de difamação, calúnia e injúria. Os artigos oferecem mecanismos legais para que indivíduos possam buscar reparação em casos de violações desses direitos. Os dispositivos reforçam a proteção contra ataques à reputação e integridade moral que podem atingir também pessoas públicas, a exemplo das mulheres que exercem cargos políticos, citadas em outros momentos neste livro.

6.2 Imagens íntimas não consentidas

A exposição das imagens pessoais nas diversas mídias é uma preocupação recorrente no âmbito da Internet. Durante os debates de elaboração do Marco Civil da Internet, casos de **"revenge porn"**, ou, pela conceituação mais apropriada, **"disseminação de imagens íntimas não consentidas"**, foram levantados para que houvesse mais celeridade no monitoramento e na remoção por parte dos provedores de aplicações. Assim, o **artigo 21 do MCI** foi elaborado de modo a trazer um regime de **"notificação e retirada"** (*notice and takedown*), segundo o qual os provedores são subsidiariamente responsáveis quando, mediante uma notificação da vítima o seu representante legal, não promove de forma diligente a retirada do conteúdo que veicula cenas de nudez ou de atos sexuais de caráter privado.

Além do MCI, a **Lei nº 12.737/2012**, conhecida como **Lei Carolina Dieckmann**, um marco significativo no combate à disseminação não consentida de imagens íntimas no Brasil. Introduzida após a atriz Carolina Dieckmann ter suas fotos pessoais divulgadas sem autorização, a legislação alterou o Código Penal para criminalizar explicitamente a **invasão de dispositivos eletrônicos com o intuito de obter, adulterar ou destruir dados, incluindo imagens íntimas**. A lei buscou preencher lacunas existentes até então no ordenamento jurídico brasileiro, proporcionando uma resposta mais eficaz diante dos crescentes casos de violação da privacidade digital. Sua aprovação representou um esforço legal para adequar a legislação às transformações tecnológicas e proteger a intimidade das pessoas em um contexto digital cada vez mais presente em nossas vidas.

A aprovação desse projeto na Câmara e o subsequente debate no Senado destacam o esforço legislativo em responder aos desafios impostos pelos avanços na IA, particularmente no que se refere à proteção da privacidade e da dignidade das pessoas no ambiente digital. Essa medida legislativa é um passo importante na luta contra a disseminação de conteúdo íntimo não consentido, buscando proteger a integridade e a privacidade das vítimas desses crimes.

O enfrentamento das chamadas **deep nudes**, contudo, requer uma abordagem coordenada, para além da necessidade de legislações mais atualizadas. Relatório recente da UNESCO (2023) destaca a necessidade de mecanismos de denúncia, métodos proativos de identificação de conteúdos artificialmente criados e transparência no acesso a controles de terceiros como medidas cruciais. Por parte do desenvolvedores, é necessário exigir que as ferramentas de IA generativa de imagens imponham restrições de *prompts* (comandos), diminuindo os riscos de disseminação de pornografia de IA e desinformação, por exemplo.

Uma medida interessante é a plataforma **StopNCII (Stop Non-Consensual Intimate Image Abuse)**, operada pela Revenge Porn Helpline, que oferece ferramentas para a proteção de imagens íntimas. A organização é referência em iniciativas para o acolhimento de vítimas do compartilhamento não-consentido de imagens íntimas. A ferramenta oferecida por eles funciona por meio da criação de um *hash* - uma espécie de impressão digital - da(s) imagem(ns)/vídeo(s) íntimos, que servirá para procurar por arquivos semelhantes a esse *hash* nas bases de companhias parceiras do projeto e remover tais arquivos, impedindo que eles sejam compartilhados.

6.3 Quando a misoginia encontra a IA: deep fakes e deep nudes

Na era das tecnologias de Inteligência Artificial (IA), a preocupação com a disseminação de imagens e vídeos pessoais alcançou um novo patamar com o advento e disseminação de tecnologias de **deep fakes**. Essa técnica permite alterar não apenas imagens estáticas, mas também vídeos, áudios e até transmissões ao vivo, desafiando nossa capacidade de discernir o real do falso.

As chamadas **deep nudes** são imagens íntimas geradas por IA e representam uma ameaça significativa não apenas para figuras públicas, mas para qualquer mulher com imagens disponíveis na internet.

Recentemente, a Câmara dos Deputados aprovou o **Projeto de Lei (PL) 9930/18**, que avança o debate sobre a criminalização de "registro da intimidade sexual" sem autorização, incluindo o uso de IA para modificar imagens com a inserção de pessoas em cenas de nudez ou atos íntimos. A proposta, de autoria da deputada Erika Kokay (PT-DF), aumenta a pena para quem for condenado por esse crime, que passaria de seis meses a um ano de prisão para um a quatro anos, além de multa.

O que é “Deep fake”?

“...trata-se de uma técnica de I.A. que permite a criação de vídeos e imagens realistas de pessoas que não existem ou de pessoas reais, fazendo parecer que elas disseram ou fizeram coisas que nunca foram ditas ou feitas, de fato.”

FONTE: Stela Maris Fernandes Pereira 30/12/22 para o Politize!
<https://bitly.ws/36G6N>

Caso 4. *Deep nudes* e violência política de gênero e raça contra Diane Rwigara

Diane Rwigara, única mulher candidata à presidência de Ruanda, enfrentou desafios significativos em sua campanha eleitoral. Após anunciar sua candidatura, ela se tornou alvo de ataques online orquestrados pelo partido governista, o Rwandan Patriotic Front (RPF), liderado pelo presidente Paul Kagame. **Fotos nuas falsificadas de Rwigara foram postadas na internet, o que ela afirmou ser uma tática para silenciá-la.**



Além dos ataques e trolling online sofridos por Rwigara, ela relatou que seus apoiadores também foram ofendidos e censurados. Apesar de Ruanda ter o maior número de legisladoras femininas no mundo, Rwigara enfrentou obstáculos significativos como candidata à presidência. Algumas semanas após o incidente com as fotos, ela foi desqualificada pela comissão eleitoral do país, acusada de fraude eleitoral por supostamente submeter nomes de pessoas falecidas como apoiadoras. Rwigara negou as acusações, afirmando que eram mentiras fabricadas.

A desqualificação de Rwigara destaca os desafios enfrentados por candidatas femininas em Ruanda, apesar da alta representação feminina no parlamento. Em resposta à desqualificação e adversidades enfrentadas, ela se voltou para o ativismo de direitos humanos, fundando o grupo ativista People Salvation Movement.

Para mais informações sobre este caso, acesse: <https://edition.cnn.com/2017/08/04/africa/rwanda-election-nude-photos-candidate/index.html>. (em inglês)

6.4 Como lidar com disseminação de imagens íntimas ou produzidas por IA?

A proteção ao direito de imagem, considerado um bem jurídico inviolável e indisponível, encontra respaldo no art. 5º, inciso X, da Constituição Federal de 1988 e no art. 20, do Código Civil de 2002. Conforme já mencionado, esses dispositivos legais destacam a importância de proteger a imagem das pessoas como um componente essencial de sua dignidade. Para endereçar a disseminação de imagens íntimas não consentidas, além da **Lei Carolina Dieckmann**, mais recentemente, a **Lei de Importunação Sexual** (Lei n. 13.718/2018) alterou o Código Penal brasileiro, inserindo o artigo **218-C** sobre divulgação de cena de estupro ou de cena de estupro de vulnerável, de cena de sexo ou de pornografia. Em seu § 1º, há previsão de aumento de pena quando o criminoso mantém ou tenha mantido relação íntima de afeto com a vítima ou com o fim de vingança ou humilhação.

Caso tenha tido suas imagens íntimas compartilhadas sem o seu consentimento, tente colher provas como capturas de tela, depoimentos ou confissões e procure a orientação de um advogado para saber a melhor maneira de registrar a ocorrência.

Artigo 218-C, CP. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de estupro: Pena - reclusão, de 2 (dois) a 5 (cinco) anos.

6.5 Desinformação generificada e violência política

Apesar de avanços recentes, a representação feminina na política brasileira continua baixa. Atualmente, há apenas 18,5% de mulheres no Senado e 17,7% na Câmara dos Deputados. No âmbito municipal, de acordo com pesquisa do **Instituto Alziras (2022)**, apenas 12% dos municípios têm prefeitas, sendo apenas 4% delas mulheres negras. A **violência política de gênero** contribui para essa desigualdade, representando 36% dos casos de violência política entre 2020 e 2022. Ela afeta, principalmente, as mulheres negras e representantes LGBTQIA+.

De acordo com o projeto MonitorA (2020 e 2022), a **violência política de gênero online** frequentemente ganha contornos de assédio, insultos e ataques com estereótipos de gênero, e coloca em questão os limites da liberdade de expressão. Ainda que a liberdade de expressão seja um direito fundamental, ela não abarca o direito de **difamar, assediar** ou **ameaçar** outrem. Portanto, ações que visam **silenciar** ou **intimidar** candidatas com base em gênero ou raça ultrapassam os limites aceitáveis da livre expressão.

De acordo com Curzi (2021), em relação às campanhas de desinformação, "estudos conduzidos em diversos países (...) mostram que ataques contra mulheres e pessoas LGBTQIA+ são frequentemente conectados a estereótipos relacionados a suas identidades de gênero ou orientação afetiva". Nesse sentido, como estratégia de afetação de suas campanhas, emerge o fenômeno da **desinformação generificada, que vai além da disseminação de informações falsas, incorporando e amplificando narrativas de gênero preexistentes para reforçar estereótipos e preconceitos.**

O objetivo da desinformação generificada não se restringe a prejudicar individualmente as candidatas, mas também dissuadir ativamente a participação feminina na política. Esse tipo de desinformação é uma tática direcionada que busca enfraquecer as instituições democráticas e limitar a diversidade de vozes na esfera pública.

De acordo com o **Instituto Alziras (2022)**, cerca de 58% das prefeitas brasileiras afirmam ter sofrido assédio ou violência política, com 74% enfrentando divulgação de informações falsas e 66% ataques de discurso de ódio nas redes sociais.

A **Lei de Violência Política Contra Mulheres**, Lei 14.192, promulgada em 4 de agosto de 2021, surgiu com o objetivo de criminalizar esse tipo de conduta e é um passo importante para o combate à desigualdade na política. No entanto, tal legislação tem sofrido críticas significativas em relação a falta de mecanismos de prevenção além da falta de tipificação sobre este tipo de violência para além da desinformação.

Em busca de alternativas práticas para lidar com a disseminação de imagens íntimas não consentidas, entre outros crimes cibernéticos, alguns canais de atendimento com foco em mulheres, crianças, adolescentes, entre outros grupos que costumam estar em maior vulnerabilidade nas redes, podem ser úteis para prevenir e orientar sobre medidas de segurança online:

- Caso tenha tido sua intimidade indevidamente exposta, ou caso acredite que tenha sofrido qualquer outro tipo de violação dos seus direitos fundamentais, é possível buscar orientação através do chat ou por meio de ligação de canais como o *Safer Net*: <https://new.safernet.org.br/helpline>
- Iniciativas como esta devem garantir que as suas informações compartilhadas sejam mantidas em sigilo. Uma das principais formas de ter essa garantia é com a criptografia dos meios de comunicação entre a vítima e profissionais orientadores.

Caso 5. Manuela d'Ávila e campanhas de desinformação generificada

Manuela d'Ávila, jornalista e ex-deputada federal, tem enfrentado desafios significativos devido à **desinformação** e **ataques virtuais**. Ela revelou que foi repetidamente agredida em locais públicos devido a mentiras espalhadas sobre ela, inclusive afetando a sua filha. Esses ataques, e o medo por sua segurança e de sua família, motivaram sua decisão de não se candidatar nas eleições de 2022.



Desde que começou a concorrer a cargos políticos, Manuela se tornou alvo frequente de notícias falsas, que se intensificaram em 2018, quando foi candidata à vice-presidência. Ela foi falsamente acusada de diversas coisas, inclusive de ligar para o homem que esfaqueou Jair Bolsonaro, e teve sua imagem manipulada em montagens ofensivas por diversas vezes. Sua família também sofreu com a desinformação: quando Manuela estava grávida, falsas alegações sobre gastos irregulares com dinheiro público foram disseminadas; após o nascimento de sua filha, Laura, detalhes do parto foram divulgados sem consentimento e a criança chegou a sofrer agressão física.

Manuela destaca que o sistema de desinformação é amplo e envolve diversos setores da sociedade, incluindo a imprensa, que muitas vezes se omite diante desses ataques. Suas experiências demonstram os impactos severos da desinformação na vida política, especialmente para mulheres, e a necessidade urgente de medidas para combater esse fenômeno.

Fonte:

<https://desinformante.com.br/atingidas-pela-desinformacao-manuela-davila/>

7. Recomendações para o setor público

A garantia de ambientes digitais mais seguros depende fundamentalmente de ação direta do setor público e parcerias deste com o setor privado. Apesar da falta de regulação específica, órgãos públicos — como o Ministério da Justiça e da Segurança Pública, o Ministério de Direitos Humanos, o Ministério da Igualdade Racial e o Ministério das Mulheres, além de Secretarias específicas, como a Secretaria de Comunicação Social (Secom) e a Secretaria Nacional do Consumidor (Senacon) — podem, efetivamente, adotar medidas e desenvolver políticas públicas para aumentar a qualidade e a segurança dos espaços online.

Neste contexto, iniciativas como a recente **colaboração entre a Secretaria Nacional de Segurança Pública (Senasp) e a Senacon** são exemplos da atuação governamental para enfrentar os desafios de crimes cibernéticos e proteger os direitos dos usuários. Esta parceria entre pastas é estratégica para estabelecer um **monitoramento** eficaz de atividades ilícitas online e fortalecer a segurança digital. A troca de informações e a coordenação entre diferentes órgãos do governo possibilitam uma resposta mais rápida e assertiva às ameaças digitais, incluindo a disseminação não consentida de imagens íntimas e outros tipos de violência de gênero online. Mesmo sem uma lei de regulação das plataformas no Brasil, é possível dar maior materialidade para a implementação no contexto digital de políticas públicas e outras normas específicas já existentes, como a **Lei Maria da Penha e a Lei de Violência Política Contra Mulheres**.

Ainda que seja relevante tipificar especificamente as violências online, seguindo a recomendação da **Relatoria Especial da ONU sobre Violência contra Mulheres e Meninas (A/HRC/38/47)**, os Estados devem não apenas punir a violência de gênero online, mas agir para a sua prevenção de forma ativa.

A concepção de **programas para a conscientização** e medidas voltadas à capacitação técnica de autoridades sobre a proteção contra tais violências é um passo vital para a garantia de ambientes digitais mais seguros. Ademais, é necessário equipar as **polícias e agências de inteligência** com treinamento específico, multidisciplinar e capacitação técnica para oferecer tratamento adequado às vítimas, coletar de forma mais célere as provas nos meios digitais e responder efetivamente aos casos denunciados.

Além destes pontos, a **colaboração com o setor privado** é essencial, devido à escala de conteúdo, a transnacionalidade e a reprodutibilidade, características típicas das plataformas digitais. A criação de canais de denúncia e suporte acessíveis e eficientes, que permitam às vítimas relatar casos de violência e buscar ajuda, é uma ação concreta que combina os esforços do setor público e privado. Esses canais podem incluir linhas diretas, plataformas online e aplicativos móveis que facilitam a comunicação entre as vítimas, as autoridades e as organizações de apoio.

Por fim, a cooperação para o desenvolvimento de tecnologias de monitoramento e filtragem também é fundamental. O setor público pode colaborar com empresas de tecnologia para aprimorar a contextualização da moderação de conteúdo.

Destacamos as seguintes ações:

1. Desenvolvimento de uma legislação específica: promover a criação de lei que aborde diretamente a **violência política de gênero e raça online**. A lei precisa definir claramente o que constitui violência online, estabelecer obrigações para as plataformas digitais na prevenção e no combate a esses atos, e determinar penalidades para o descumprimento.

2. Fortalecer mecanismos de fiscalização: é necessário estabelecer órgãos reguladores, ou fortalecer os já existentes, com a autoridade e os recursos necessários para monitorar as plataformas digitais, garantindo que cumpram as normativas relacionadas à violência política de gênero e raça e efetivem a proteção às candidatas.

3. Criação de um conselho multissetorial: recomenda-se a criação de um Grupo de Trabalho Permanente para Direitos Humanos e Novas Tecnologias, com atuação interministerial, constituído por representantes de empresas de tecnologia, do terceiro setor, do governo e da academia, para desenvolver estratégias conjuntas no combate à violência política de gênero e raça. A estratégia inclui a criação de campanhas de conscientização e a colaboração no desenvolvimento de ferramentas de moderação de conteúdo.

4. Investir em educação midiática e conscientização: implementar programas educacionais e campanhas de conscientização nacionais sobre a natureza e os impactos da violência política de gênero e raça online. Essas iniciativas podem visar tanto o público em geral quanto grupos específicos, como jovens, educadores e profissionais da área de tecnologia.

5. Apoio à pesquisa e desenvolvimento: financiamento de pesquisas sobre a violência política de gênero e raça em ambientes digitais e sobre o impacto das políticas de moderação de conteúdo a partir de editais específicos, para ajudar a entender melhor o problema e a desenvolver soluções tecnológicas mais eficazes.

6. Canais de denúncia e suporte: estabelecer e divulgar canais acessíveis e eficientes para que vítimas de violência política de gênero e raça possam denunciar incidentes e buscar apoio.



8. Recomendações para o setor privado

As grandes empresas de tecnologia precisam assumir responsabilidades para a promoção e respeito aos direitos humanos, seguindo os recentes esforços de recomendação da **Relatoria Especial da ONU para a Liberdade de Expressão e Opinião** e os **United Nations Guiding Principles on Business and Human Rights (UNGP)**. O compromisso com a democracia exige que medidas sejam adotadas para a mitigação e combate adequado à violência política de gênero e raça.

Recomendamos as seguintes iniciativas:

1. Implementar políticas de moderação de conteúdo

consistentes e efetivas: desenvolver e aplicar políticas claras sobre o que constitui violência política de gênero e raça, e como tais conteúdos serão tratados, incluindo a remoção rápida de conteúdos ofensivos ou prejudiciais.

2. Transparência nas práticas de moderação: indicar quais os critérios usados para avaliar e remover conteúdos, bem como as medidas tomadas como respostas às violações. O detalhamento das ações implementadas pode ser feito por meio de relatórios semestrais, por exemplo.

3. Moderação contextualizada: alocar recursos para o desenvolvimento de tecnologias de IA que possam identificar e filtrar conteúdos de violência política de gênero e raça de maneira eficiente a partir da colaboração com agências e organizações locais.

4. Capacitação e diversificação da equipe de moderação:

garantir diversidade e treinamento das equipes responsáveis pela moderação de conteúdo para entender e identificar adequadamente nuances relacionadas a gênero e raça.

5. Canais de denúncia acessíveis: criar e manter canais de fácil acesso e utilização para que os usuários possam denunciar conteúdos ou comportamentos abusivos relacionados à violência política de gênero e raça.

6. Criação de Conselho de Segurança Digital: conselhos constituídos por especialistas e representantes do terceiro setor e da academia podem ser frutíferos para a melhor compreensão de dinâmicas da violência online, incluindo a violência política de gênero e raça. Além disso, podem fornecer valiosas contribuições para o aprimoramento das políticas e práticas de moderação de conteúdo.

7. Educação e conscientização dos usuários: desenvolver e promover campanhas educativas para informar os usuários sobre a violência política de gênero e raça e incentivá-los a adotar comportamentos online responsáveis e respeitosos.

8. Avaliação contínua e melhoria das políticas: monitorar regularmente a eficácia das políticas e práticas implementadas, além de estar aberto a fazer ajustes com base no *feedback* dos usuários e tendências sociais.

9. Monitoramento intensificado durante eleições: aumentar o monitoramento de conteúdos relacionados às eleições, com foco especial na violência política de gênero e raça, para responder rapidamente a quaisquer problemas que possam surgir no período.

Considerações finais

Este livro é um esforço voltado à difusão de conhecimento sobre os desafios complexos do cenário digital contemporâneo. Tendo como foco debates cruciais relacionados à construção de um ambiente virtual democrático e inclusivo, a publicação procuramos destacar questões fundamentais como censura na Internet, crimes de ódio, ameaças à violência física, perseguição, exposição de dados pessoais e uso indevido da imagem. Por fim, buscamos apresentar recomendações de ações e orientações para vítimas, além de seus representantes legais, bem como para os setores público e privado para a promoção de ambientes digitais seguros e democráticos.

Oferecemos orientações práticas sobre como usuários, especialmente mulheres na política, podem lidar com situações abusivas online, levando em consideração a legislação vigente e possíveis responsabilizações. Além disso, procuramos desmistificar a percepção equivocada de que crimes digitais são menos graves, enfatizando os impactos reais na saúde mental e física das vítimas.

No contexto da liberdade de expressão, procuramos explorar como o ordenamento jurídico brasileiro lida com a censura online, destacando o papel do Marco Civil da Internet e do Projeto de Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet (PL 2.630/2020). Foi ressaltada a necessidade de aprimorar a legislação para garantir a proteção efetiva da liberdade de expressão diante das novas formas de censura digital.

Entendendo que cenários menos violentos no mundo virtual não dependem apenas das legislações, enfatizamos a necessidade de combiná-las com boas práticas por parte dos provedores de aplicações e políticas públicas informadas e eficientes. Também destacamos que as lacunas legais, evidentes não apenas devido ao avanço das novas tecnologias, mas também pelas barreiras de acesso e intervenção ativa de mulheres e minorias na formulação de políticas públicas, produzem gargalos para a proteção e fruição dos direitos humanos destes grupos.

Respostas mais eficazes, por parte das instituições públicas e das plataformas, se tornam **ainda mais essenciais no contexto das eleições**. É diante desse cenário complexo que procuramos fornecer conhecimento legal para o enfrentamento dos desafios da violência política de gênero e raça online, contribuindo para a construção de um ambiente digital mais inclusivo, seguro e democrático.

O presente livro, ao explorar a violência política influenciada por gênero e raça, ressalta uma questão fundamental para o alcance do Objetivo de Desenvolvimento Sustentável 5 (ODS 5) - Igualdade de Gênero. Esta análise destaca a urgência de enfrentar as formas específicas de violência que mulheres, especialmente aquelas de grupos raciais e étnicos marginalizados, enfrentam no âmbito político. A erradicação dessas formas de violência é essencial para garantir a plena participação das mulheres em igualdade de condições na vida política e pública, conforme estabelecido pelos alvos do ODS 5. Além disso, reconhece-se que a superação dessa violência contribui para a criação de sociedades mais justas e inclusivas, onde as decisões políticas refletem a diversidade e a riqueza de todas as suas vozes, alinhando-se diretamente com o compromisso global de promover a igualdade de gênero e empoderar todas as mulheres e meninas.

Referências bibliográficas

ARAÚJO, João. Em novo relatório, MonitorA 2022 analisa violência política de gênero nas eleições de 2022.

InternetLab, 23 maio 2023. Disponível em:

<https://internetlab.org.br/pt/noticias/monitora-2022-confira-o-relatorio-na-integra/>

ANPD; TRIBUNAL SUPERIOR ELEITORAL. Guia Orientativo: Aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) por agentes de tratamento no contexto eleitoral.

Brasília: TSE, 2021. Disponível em:

https://www.gov.br/anpd/pt-br/assuntos/noticias/guia_lgpd_final.pdf.

BRASIL. Presidência da República. Secretaria-Geral. Subchefia para Assuntos Jurídicos. Lei nº 13.642, de 3 de abril de 2018. Disponível em:

https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13642.htm.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Lei nº 12.737, de 30 de novembro de 2012. Disponível em:

https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm.

BRASIL. Presidência da República. Secretaria-Geral. Subchefia para Assuntos Jurídicos. Lei nº 14.132, de 31 de março de 2021. Disponível em:

https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14132.htm.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. Difamação - Art. 139. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1225916#:~:text=139.,a%20um%20ano%2C%20e%20multa.

BRASIL. Presidência da República. Secretaria-Geral. Subchefia para Assuntos Jurídicos. Lei nº 14.532, de 11 de janeiro de 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/lei/l14532.htm.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Lei nº 7.716, de 5 de janeiro de 1989. Dispõe sobre crimes resultantes de preconceito de raça ou de cor. Brasília, DF: Presidência da República, Casa Civil, Subchefia para Assuntos Jurídicos, 1989. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l7716.htm.

BRASIL. Decreto-Lei 2.848, de 07 de dezembro de 1940. Código Penal. Diário Oficial da União, Rio de Janeiro, 31 dez. 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm.

BRASIL. Constituição da República Federativa do Brasil. Promulgada em 5 de outubro de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm.

BRASIL. Senado Federal. Projeto de Lei no 2.630, de 2020, do Senador Alessandro Vieira, que institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet. Brasília, DF: Senado Federal, 2020a. Disponível em: https://legis.senado.leg.br/sdleg_getter/documento?dm=8110634&ts=1685643474170&disposition=inline&_gl=1*1mu f8kn*_ga*MjQ2MTI0NjcuMTY4NjE4MjU2MQ..*_ga_CW3ZH25XMK*MTY4NjE4MjU2MS4xLjAuMTY4NjE4MjU2MS4wLjAuMA.

BRASIL, Lei nº 12.965 de 23 de abril de 2014. Marco Civil da Internet. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

BRASIL. Câmara dos Deputados. Projeto de Lei no 2.630, de 2020, do Senador Alessandro Vieira, que institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet, aprovado pelo Senado e enviado à Câmara. Brasília, DF: Câmara dos Deputados, 2020b. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1909983.

BRASIL. Câmara dos Deputados. Substitutivo do Projeto de Lei no 2.630, de 2020, do Senador Alessandro Vieira, que institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet, apresentado à Câmara pelo relator, o deputado Orlando Silva em 31 de março de 2022. Brasília, DF: Câmara dos Deputados, 2022. Disponível em: <https://www.camara.leg.br/midias/file/2022/03/fake.pdf>.

BRASIL. Lei nº 14.532, de 11 de janeiro de 2023. Lei que altera a Lei nº 7.716, de 5 de janeiro de 1989 (Lei do Crime Racial), e o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal). Disponível em:

https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/lei/l14532.htm.

BRASIL. Supremo Tribunal Federal. Mandado de Injunção 4.733 Distrito Federal. Relator: Min. Edson Fachin. Ementa: Direito Constitucional. Disponível em:

<https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=753957476>

BRAGA, Alex. Janja diz que posts são 'machistas e criminosos' após ter conta hackeada em rede social. Terra, 2023. Disponível em:

<https://www.terra.com.br/noticias/brasil/politica/janja-diz-que-posts-sao-machistas-e-criminosos-apos-ter-conta-hackeada-em-rede-social,982de58d07d70d93853f798977d05a40r7vpvcb1.html>.

BELLI, Luca; ZINGALES, Nicolo; CURZI, Yasmin (Eds.). Glossary of platform law and policy terms. Rio de Janeiro: FGV Direito Rio, 2021. Disponível em:

<https://repositorio.fgv.br/server/api/core/bitstreams/1064b8ef-7d47-44be-9413-174681575745/content>

BUSARI, Stephanie; IDOWU, Torera. Fake nude photos were used to 'silence me', disqualified Rwandan candidate says. CNN, 5 de agosto de 2017. Disponível em: <https://edition.cnn.com/2017/08/04/africa/rwanda-election-nude-photos-candidate/index.html>.

CÂMARA DOS DEPUTADOS. Projeto de Lei 9930/2018. Autora: Erika Kokay. Criminaliza a divulgação, sem consentimento, de foto, vídeo ou outros materiais relativos à intimidade de mulher, modificando o Decreto-Lei nº 2.848, de 7 de dezembro de 1940, Código Penal. Aprovada com alterações no Plenário em 07/12/2023. Nova redação. Disponível em: <https://www.camara.leg.br/propostas-legislativas/2170680>.

CODING RIGHTS; INTERNETLAB. Violências de gênero na internet: diagnóstico, soluções e desafios. Contribuição conjunta do Brasil para a relatora especial da ONU sobre violência contra a mulher. São Paulo, 2017.

CURZI, Yasmin. Disinformation (Gendered). In Belli, L.; Zingales, N. & Curzi, Y. (Eds.), Glossary of Platform Law and Policy Terms (online). FGV Direito Rio. 2021. <https://platformglossary.info/disinformation-gendered/>

CURZI, Yasmin. I silenced myself: Brazilian Female Perspectives on OGBV
In: Feminist perspectives on social media governance. ITFC, 2023.

CURZI, Yasmin; ZINGALES, Nicolo; GASPAR, Walter Britto; LEITÃO, Clara; COUTO, Natália; REBELO, Leandro & OLIVEIRA, Maria Eduarda. Nota técnica do Centro de Tecnologia e Sociedade da FGV Direito Rio sobre o substitutivo ao PL 2.630/2020. Rio de Janeiro: FGV Direito Rio, 2021. Disponível em: <https://bibliotecadigital.fgv.br/dspace/handle/10438/31348>.

DUNN, Suzie, Technology-Facilitated Gender-Based Violence: An Overview (December 7, 2020). Suzie Dunn, "Technology-Facilitated Gender-Based Violence: An Overview" (2020) Centre for International Governance Innovation: Supporting a Safer Internet Paper No. 1., Available at SSRN: <https://ssrn.com/abstract=3772042>

FACULDADE BAIANA DE DIREITO; JUSBRASIL. Racismo e Injúria Racial Praticados nas Redes Sociais: Relatório do Observatório das Condenações Judiciais em 2ª Instância até o ano de 2022. Salvador/BA, outubro 2023. Disponível em: <https://www.conjur.com.br/dl/pe/pesquisa-racismo-redes-2023.pdf>.

GARBIN, Luciana. Chats que vetam presença de mulheres se multiplicam na internet: é a praga dos 'chans'. Estadão, São Paulo, 27 set. 2023, 20h. Disponível em: <https://www.estadao.com.br/cultura/luciana-garbin/chans-com-crimes-e-discursos-de-odio-contra-mulheres-se-multiplicam-na-internet/>.

HAGGART, Blayne et KELLER, Clara Iglesias. Democratic legitimacy in global platform governance. Telecommunications Policy, 2021, vol. 45, no 6, p. 102 - 152.

INSTITUTO ALZIRAS; OXFAM BRASIL. Desigualdades de Gênero e Raça na Política Brasileira. Publicado em 24 de julho de 2022. Disponível em:

<https://cms.alziras.org.br/uploads/DESIGUALDADES%20DE%20G%20C3%8ANERO%20E%20RA%20C3%87A%20NA%20POL%20C3%8DTICA%20BRASILEIRA.pdf>

Inter-parliamentary Union for democracy. Sexism, Harassment and violence against women in parliaments in Africa. Novembro de 2021. Disponível em:

<https://www.ipu.org/resources/publications/issue-briefs/2021-11/sexism-harassment-and-violence-against-women-in-parliaments-in-africa>

NAGLE, Angela (2017) Kill All Normies: Online Culture Wars from 4chan and Tumblr to Trump and the Alt-Right. Winchester: Zero Books.

ONU Women, 2021. Violence against women in the online space: Insights from a multi-country study in the Arab States - Summary report. Disponível em:

https://arabstates.unwomen.org/sites/default/files/Field%20Office%20Arab%20States/Attachments/Publications/2021/11/Summary_Keyfindings_Final_EN.pdf.

OLIVA, Thiago Dias; ANTONIALLI, Denny Marcelo; SANTOS, Maíke Wile dos. Censura Judicial ao Humor: Análise de Decisões Judiciais Envolvendo Liberdade de Expressão na Internet. Revista Direitos Culturais, Santo Ângelo, v. 14, n. 34, p. 19-44, maio/agos. 2019. Disponível em:

<https://www.internetlab.org.br/wp-content/uploads/2019/05/2914-10535-1-PB.pdf>

PARLAMENTO EUROPEU. A Lei dos Mercados Digitais e da Lei dos Serviços Digitais da UE em detalhe. 2021. Disponível em:

<https://www.europarl.europa.eu/news/pt/headlines/society/20211209STO19124/a-lei-dos-mercados-digitais-e-da-lei-dos-servicos-digitais-da-ue-explicadas>

Plan International. 2020. Libres d'être en ligne ? Les expériences des filles et des jeunes femmes en matière de harcèlement en ligne. La situation des filles dans le monde. Disponível em: <https://plan-international.org/uploads/2023/06/SOTWGR2020-CommsReport-edition2023-FR.pdf>.

RAMOS, Matheus. Mais de 56 mil denúncias de stalking foram registradas no Brasil em 2022, aponta pesquisa. NP, 2023. Disponível em: <https://noticiapreta.com.br/mais-de-56-mil-denuncias-stalking-registradas-brasil-2022-aponta-pesquisa/>.

SENADO FEDERAL; Senador Alessandro Vieira. Relator: Deputado Orlando Silva. Parecer proferido em plenário ao projeto de lei nº2.630, de 2020, e apensados. Disponível em: <https://static.poder360.com.br/2023/04/pl-fake-news-camara.pdf>

TRIBUNAL DE JUSTIÇA DO DISTRITO FEDERAL E DOS TERRITÓRIOS. Calúnia. Art. 138. Disponível em: <https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/direito-facil/edicao-semanal/dos-crimes-contra-a-honra#:~:text=138%20%2D%20Caluniar%20algu%C3%A9m%2C%20imputando%2D,imputa%C3%A7%C3%A3o%2C%20a%20propala%20ou%20divulga.>

KIM, R. Unacceptable: Responding to Technology-Facilitated Gender-Based Violence. 2021. Women's Legal Education & Action Fund (LEAF). Machine-Readable Text. Toolkit. Disponível em: <https://www.leaf.ca/factsheet/unacceptable-responding-to-technology-facilitated-gender-based-violence/>

Outros materiais relevantes

[Delegacia de cibercrimes](#) - SaferNet

[Infográfico: como denunciar sextorsão?](#) - SaferNet

[Falando sobre ataques online e trolls - Um guia para jornalistas e criadores de conteúdo na internet.](#) - InternetLab

[Achearegra](#) - Encontre os termos de uso das principais plataformas digitais. - InternetLab

[Aumente sua segurança digital](#) - Data Labe

[AzMina publica política de uso de Inteligência Artificial](#) - Azmina

