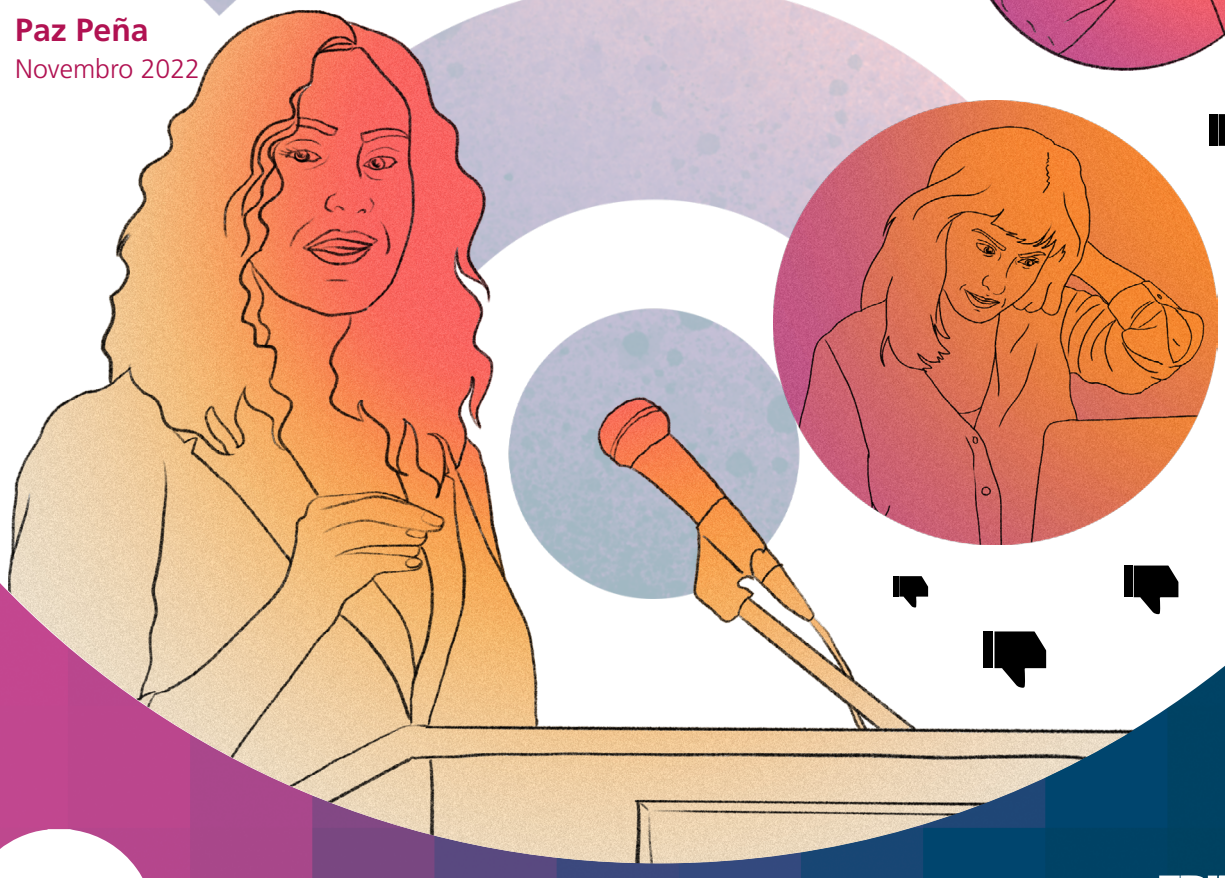
TRABALHO E JUSTIÇA SOCIAL

GUIA PRÁTICO CONTRA A VIOLÊNCIA POLÍTICA DE GÊNERO DIGITAL

Paz Peña

Novembro 2022

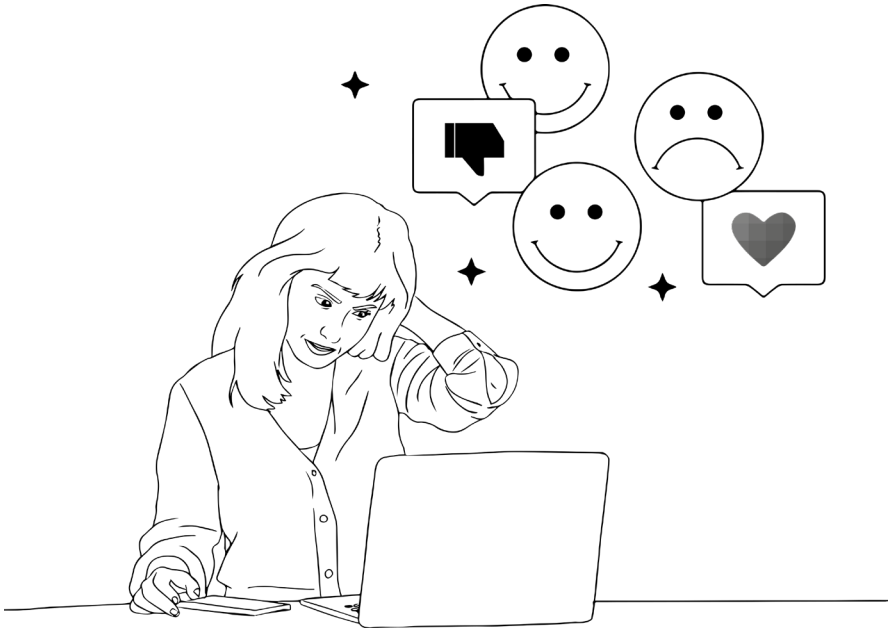


FESMINISMOS

#TOMAPARTIDO

FRIEDRICH EBERT STIFTUNG

Índice



Introdução

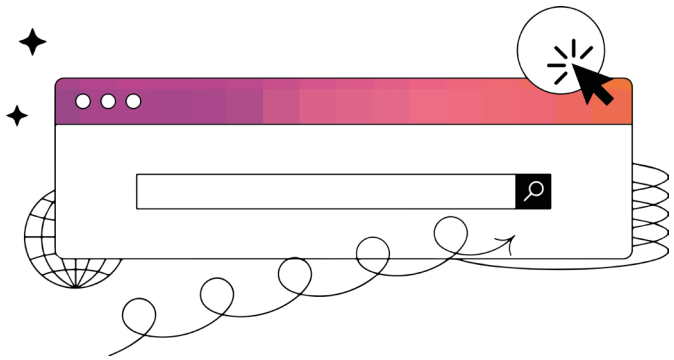
Este é um guia que visa fornecer recomendações abrangentes a pessoas e organizações que enfrentam a violência política de gênero digital e, em particular, busca integrar recomendações de segurança digital que, do ponto de vista feminista, possam enfrentar esses ataques em especial. Por se tratar de um assunto complexo que requer uma abordagem com múltiplas perspectivas, o guia está dividido em duas partes. A primeira parte é dedicada, por um lado, a um olhar de contextualização geral sobre a violência política digital baseada no gênero, que não pretende ser uma coleção completa de evidências, mas sim revisar o que sabemos sobre o problema, especialmente em América latina. Por outro lado, é também feita uma revisão das diferentes respostas que existem ao problema, um ampla gama que vai da segurança digital feminista à denúncia direta às plataformas online onde ocorrem os ataques, denúncia legal, além de outras ações de influência.

A segunda parte funciona como um anexo da primeira, pois se concentra nas ações de segurança digital que podem ser aplicadas de acordo com os tipologia de ataques mais comuns sofridos na esfera digital com base no gênero. Além disso, integra uma série de recursos externos que podem ser muito úteis para pessoas que desejem saber mais sobre segurança digital em particular.

É um trabalho que visa enfatizar a ideia de que os hábitos de segurança digital são importantes, mas não são o suficiente para enfrentar, como único trunfo, um problema estrutural, como é o caso da violência de gênero. Nesse sentido, este documento espera ser não apenas um guia de acompanhamento, mas também um catalisador de atividades coletivas que sirvam para resistir e agir contra esses ataques.

PRIMEIRA PARTE:

GUIA PRÁTICO CONTRA A VIOLÊNCIA POLÍTICA DE GÊNERO DIGITAL



Definição

Segundo a relatora especial da Organização das Nações Unidas (ONU) contra a violência contra a mulher em relatório especial sobre o tema[1], a violência política contra as mulheres inclui qualquer ato de violência de gênero, ou sua ameaça, que resulte ou possa resultar em dano ou sofrimento físico, sexual ou psicológico, e seja dirigido contra as mulheres na política por causa de sua condição de mulher ou afete as mulheres de forma desproporcional, afetando-as em períodos eleitorais, e mesmo além deles.

Esse tipo de violência pode assumir diversas formas, inclusive as perpetradas por meios digitais. Em um relatório específico sobre violência online contra mulheres, o Relator Especial da ONU[2] já havia destacado que as mulheres na política são periodicamente vítimas de violência online e violência facilitada pela tecnologia da informação e comunicação (TIC):

> Eles recebem ameaças online, geralmente de natureza misógina e muitas vezes sexualizada. Em última análise, a violência online contra as mulheres na política é um ataque direto à plena participação das mulheres na vida política e pública e ao gozo de seus direitos humanos. Ainda não se compreendeu completamente em que medida atores estatais e não estatais usam essa violência online para espalhar desinformação destinada a dissuadir as mulheres de participar da política, alienar o apoio popular de mulheres politicamente ativas e influenciar a maneira como homens e mulheres veem certas questões.

A digital, em sua extensão, pode representar espaços de violência[3] de gênero online contra mulheres políticas. No entanto, vários estudos têm demonstrado como as redes sociais são, em particular, espaços onde este tipo de violência é mais frequentemente exercido. Há vasta evidência de que as mulheres políticas vivenciam um volume significativamente maior de comentários sobre sua aparência e vida familiar nas redes sociais do que seus correlatos masculinos[4]. Em particular, um estudo no Chile mostra que a violência política de gênero no Twitter é realizada por meio de descrédito, menosprezo pelas capacidades e alusões ao corpo ou à sexualidade. E é feito um alerta para a necessidade de observar as agressões a partir da interseccionalidade das vítimas. Por exemplo, os ataques às indígenas candidatas à Constituinte do Chile foram principalmente racistas; por outro lado, as dissidências sexuais foram ob-

1 A73/301. 6 de agosto de 2018

2 A/HCR/38/47. 18 de junho de 2018

3 Ver Anistia Internacional (2018). TOXIC TWITTER – TRIGGERS OF VIOLENCE AND ABUSE AGAINST WOMEN ON TWITTER. Chapter 2. https://www.amnesty.org/en/latest/news/2018/03/online-violence-against-women-chapter-2-3/

4 Barboni, E. (2016). (Anti)social media: the benefits and pitfalls of digital for female politicians; Chaturvedi, 5, I Am a Troll: Inside the Secret World of the BJP's Digital Army, Juggernaut

jeto de ofensas de baixo calão por sua orientação sexual, identidade ou expressão de gênero, assim como jovens candidatas (com menos de 35 anos) e acadêmicas enfrentam níveis mais elevados de menosprezo de suas habilidades.

Além disso, a disseminação de desinformação e notícias falsas (fake news) é generalizada nessas plataformas, muitas vezes dirigidas a mulheres candidatas a cargos legislativos, mas também mulheres políticas fora dos ciclos eleitorais. Pesquisas tem demonstrado uma correlação entre a disseminação de desinformação sobre funções, campanhas, crenças e ações das mulheres na política e o assédio e abusos que recebem em função disso[5]. Em muitos casos, esses ataques são produto de uma colaboração coletiva, com a presença de "bots" e "trolls" para ampliar o número de mensagens violentas e seus efeitos. A percepção de impunidade encoraja agressores e aumenta o sentimento de insegurança e violação das mulheres, distanciando muitas delas da participação política[6].

Efeitos

As consequências da violência de gênero online são muitas vezes relativizadas devido à ideia de que online "não é real", porém, os efeitos na vida das vítimas são persistentes em diversos níveis. A relatora especial da ONU reconheceu que atos de violência online "podem levar as mulheres a abster-se de usar a Internet" (parágrafo 26), bem como danos ou sofrimento psicológico, físico, sexual ou econômico[7].

De acordo com o relatório especial de 2021 do Parlamento Europeu sobre o assunto,[8] há um impacto direto dessa violência nas vítimas e alerta para uma dimensão interseccional que também deve ser observada em conjunto com outras formas de discriminação e discurso de ódio, como os recebidos por pessoas LGBTQIA+, assim como grupos racializados, minorias, e diferentes comunidades religiosas.

O relatório sustenta ainda que o maior impacto da violência de gênero online é no nível mental, o que se reflete em uma maior incidência de depressão e transtornos de ansiedade, com impacto na redução da qualidade de vida. Além disso, reconhece uma série de impactos econômicos, como os custos decorrentes da procura de assistência jurídica e de saúde e os riscos de perda de emprego ou menor produtividade.

Para o National Democracy Institute (NDI), há uma clara relação entre o trolling online persistente e agressivo e os ataques físicos reais que algumas mulheres enfrentam, o se que chama de "efeito passarela", e destaca o trágico exemplo do assassinato da parlamentar britânica Jo Cox pelas mãos de Thomas Mair.[9] Este último, um terrorista de direita com laços transnacionais com movimentos de supremacia branca nos Estados Unidos. Mair perseguiu Cox na Internet por muitos meses antes de matá-la, quando Cox estava visitando seu distrito eleitoral.[10]

5 Oates, Sarah and Gurevich, Olya and Walker, Christopher and Di Meco, Lucina, Running While Female: Using AI to Track how Twitter Commentary Disadvantages Women in the 2020 U.S. Primaries (August 28, 2019). http://dx.doi.org/10.2139/ssrn.3444200

6 NDI (2018). #NOTTH0ECOST Stopping Violence Against Women in Politics. Submission by the National Democracy Institute to the United Nations Special Rapporteur on Violence Against Women. https://www.ndi.org/publications/submission-national-democratic-institute-united-nations-special-rapporteur-violence

7 A/73/301. 6 de agosto de 2018

8 MEENAKSHI FERNANDES, NIOMBO LOMBA, Cecilia NAVARRA. 2021. Combating Gender based Violence: Cyber Violence. Study from the European Added Value. European Parliament. 17/03/2021 https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2021)662621

9 IND (2018). #NOTTHECOST Stopping Violence Against Women in Politics. Submission by the National Democracy Institute to the United Nations Special Rapporteur on Violence Against Women. https://www.ndi.org/not-the-cost

10 Chan, S. (2016). Right-Wing Extremist Convicted of Murdering Jo Cox, a U.K. Lawmaker. New York Times. https://www.nytimes.com/2016/11/23/world/europe/thomas-mair-convicted-murder-jo-cox.html

Soma-se a isso o impacto social da violência de gênero online, que tem efeitos nos direitos econômicos, sociais e culturais, além dos direitos humanos, das pessoas afetadas. Assim, trata-se de um fenômeno que repercute nos espaços de trabalho das mulheres, bem como em seus direitos, quando as vítimas são obrigadas a se retirar de uma plataforma como a Internet que, como tem sido reconhecido por organizações internacionais de direitos humanos,[11] é um meio fundamental para a realização dos direitos fundamentais.

Particularmente, quando essa forma de violência de gênero é recebida por mulheres políticas, contribui para gerar um ambiente hostil para o exercício pleno e igualitário dos direitos políticos das candidatas em disputa.[12] Assim, alguns efeitos no debate público são:[13]

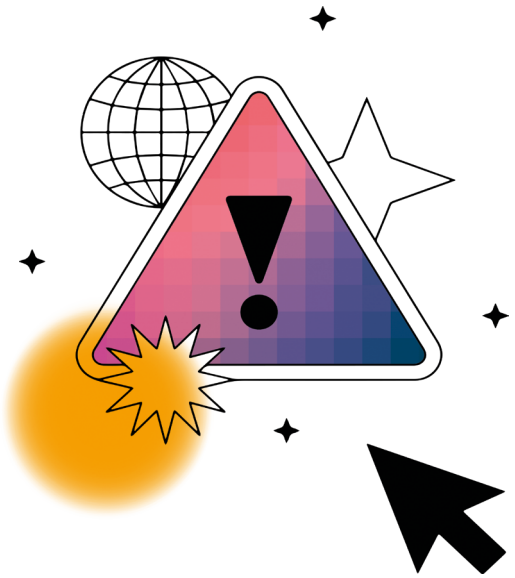
- Deslegitimar as mulheres como líderes e questionar seu direito de desempenhar funções políticas;
- Deslegitimar as mulheres como líderes e questionar seu direito de ocupar cargos políticos;
- Despersonalizar as mulheres líderes, aumentando o custo do compartilhamento de informações pessoais;
- Distrair intencionalmente as líderes para que não se concentrem no trabalho substantivo, forçando-as a gastar tempo e energia enfrentando abusos e ameaças;
- Incutir o medo pela sua segurança física e de suas famílias e obrigá-las a implementar novas medidas de segurança; e
- Desencorajar as mulheres de concorrer a eleições ou participar do debates político.

11 A/HRC/17/27 (2011)

12 Lourdes V. Barrera, Anaiz Zamora, Érika Pérez Domínguez, Ixchel Aguirre, Jessica Esculloa (2018). Violencia política a través de las tecnologías en México. Luchadoras. https://iknowpolitics.org/sites/default/files/violencia_politica_a_traves_de_las_tecnologias_contra_las_mujeres_en_mexico_pags_web.pdf

13 Atalanta (2018). (Anti)Social Media The benefits and pitfalls of digital for female politicians. https://www.atalanta.co/news-insights/antisocial-media-the-benefits-and-pitfalls-of-digital-for-female-politicians/

Tipologia de ataques comuns



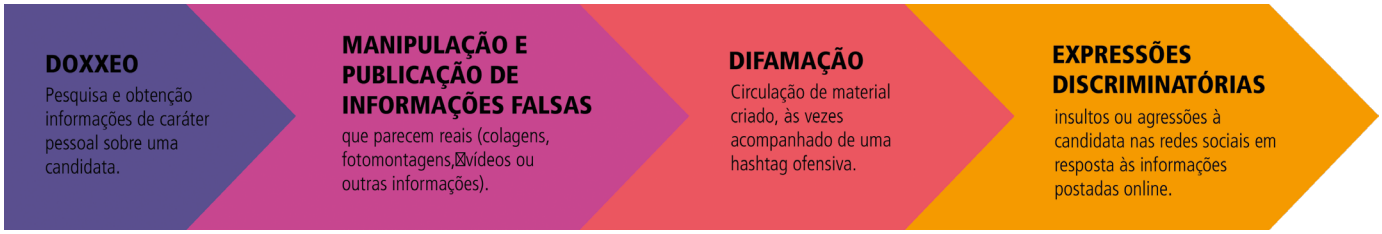
Um dos estudos mais completos da América Latina sobre violência política de gênero digital foi realizado pela Coalizão Direitos na Rede por meio de sua plataforma "Tretaqui!", que estudou o fenômeno no Brasil durante diversas campanhas eleitorais, coletando evidências de sua plataforma.[14] Neste contexto, fizeram um conjunto de seis tipos de ataques mais frequentes, com o esclarecimento de que estes tipos de ataques podem estar perfeitamente interligados um ao outro e que, muitas vezes, estão relacionados com ataques off-line.[15]

No México, a organização Luchadoras conseguiu detectar um padrão preocupante nos ataques na Internet a candidatas, o que complica e aprofunda os danos, e que revela uma intenção explícita de usar a tecnologia como ferramenta de ataque. É o que se chama de "cadeia de agressão", e que consiste em quatro situações entrelaçadas que se sucedem:

14 Ladyane Souza & Joana Varon (2020). INTERNET E ELEIÇÕES. Guia para proteção de direitos nas campanhas eleitorais. Coalizao Direitos Na Rede.

15 Existem várias formas de classificar a violência política digital baseada no gênero; Este foi escolhido apenas por ser um dos mais completos e utilizados pelas organizações da sociedade civil do continente

TIPOLOGIA DE ATAQUES	AÇÕES MAIS COMUNS
Desinformação	• Campanhas de difamação (destinadas a desacreditar a pessoa atacada). • Divulgação de informações falsas (muitas vezes ligadas à sexualidade e ao casamento).
Violações da intimidade	• Exposição de dados pessoais (conhecido como "doxxing"). • Vazamento de dados pessoais, privados e de orientação sexual. • Dados de orientação sexual coletados com ou sem consentimento ou com o consentimento por um "clique". • Compartilhamento de imagens íntimas sem consentimento (exposição de privacidade). • Uso sem consentimento de materiais e fotos. • Roubo de identidade.
Ofensas	• Discurso de ódio. • "Cyberbullying" (assédio pela internet)/insultos. • Exploração da imagem sexual e estereotipada. • Edição de imagem e vídeo.
Ameaças	• Assédio sexual e psicológico. • Assédio através da caixa de entrada nas redes sociais, com fotos e vídeos obscenos. • Perseguição. • Ameaças de violência física.
Censura	• Ataques massivos e coordenados. • Manipulação de algoritmos. • Remoção de conteúdo. • Bloqueio de postagens, páginas e perfis por denúncia ou iniciativa de redes sociais.
Invasões de privacidade	• "Zoombombing" (invasão da videoconferência ou do evento online). • Acesso não autorizado a contas ou dispositivos pessoais. • Hacking/ataques à segurança dos sistemas.



Quem provoca esses ataques?

Para as eleições de 2018, Luchadoras apurou no México que 52% dos casos de agressão a uma candidata vem de uma pessoa desconhecida, sendo os principais agressores usuários e usuárias de redes sociais, seguido por integrantes de partidos políticos; alertando que não havia informações suficientes para caracterizar os/as agressores em 33% dos casos.

Também podem ser encontradas evidências de que os ataques são produzidos no contexto de ondas de autoritarismo, misoginia e racismo em alguns países, onde as redes sociais desempenham um papel fundamental; sugere-se, inclusive, que sejam produzidos por grupos misóginos e racistas, muitas vezes organizados transnacionalmente, como os chamados grupos Incel (do inglês involutarilly celibate, involuntariamente celibatário). Agressores usam habilmente as redes sociais e sua lógica para priorizar o conteúdo que as pessoas veem, razão pela qual são até considerados tech-savvy, ou seja, têm um bom conhecimento de tecnologia.[16] Nos países latino-americanos, o uso coordenado das redes sociais contra a agenda feminista também tem sido visto por meio de discursos tóxicos e estigmatizantes.[17]

No entanto, a violência enfrentada pelas mulheres na Internet devido ao seu papel político não são incidentes isolados, mas sim uma amostra da prevalência da misoginia e da hostilidade de gênero que as mulheres encontram na rede, todos os dias.[18]

Qual é a responsabilidade das plataformas?

Ao contrário de outros tipos de violência de gênero no nível político, a que ocorre por meio das redes digitais é feita por meio de um intermediário privado: as empresas proprietárias das plataformas. No caso das plataformas de redes sociais, mas também de outras que oferecem modelos de uso gratuito, é importante examinar seu modelo de negócios, já que se baseiam na coleta de dados pessoais dos usuários, para depois perfilá-los e comercializar essas informações para terceiros. (para fins comerciais ou outros, que podem ser perfeitamente eleitorais, como demonstrado no caso da Cambridge Analytica).[19]

Em particular, como os conteúdos das redes sociais são produzidos pelos seus assinantes, para que as empresas possam obter mais dados e melhor perfilar as pessoas, é necessário que tenham a maior atenção nas plataformas (mesmo ao nível do vício).[20] e interação

16 Souza, L. & Varón, J. (2020) Violencia política de género en Internet. Policy paper América LAtina y el Caribe. Al Sur. https://www.alsur.lat/sites/default/files/2021-07/Violencia%20Pol%C3%ADtica%20de%20G%C3%A9nero%20en%20Internet%20ES.pdf

17 Chaher, S. (2021) ¿Es posible debatir en medio de discursos de odio?: activismo feminista y grupos antiderechos en el Cono Sur de América Latina. 1a ed Ciudad Autónoma de Buenos Aires: Comunicação para a Igualdad Ediciones.

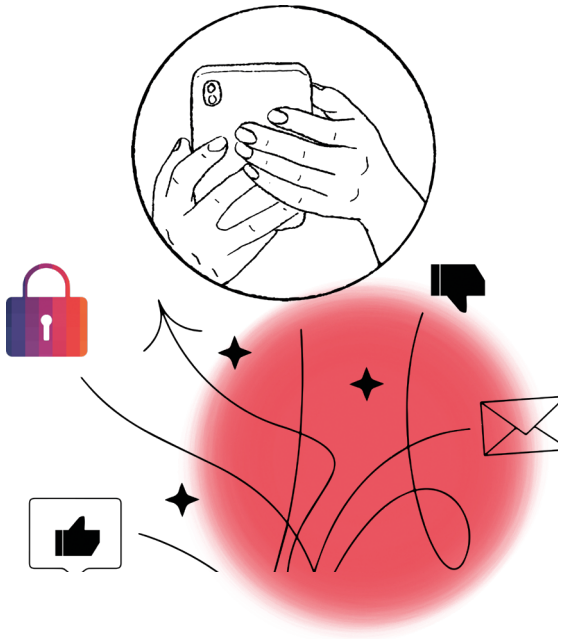
18 Barker, K. (sem data). Violence Against Women in Politics (#VAWP) – The Antithesis of (Online) Equality. The Open University Law School. https://law-school.open.ac.uk/news/violence-against-women-politics-vawp

19 BBC Mundo (2018). 5 claves para entender el escándalo de Cambridge Analytica que hizo que Facebook perdiera US$37.000 millones en un día. https://www.bbc.com/mundo/noticias-43472797

20 Al Jazeera (2021). Facebook products 'harm children, stoke division': Whistleblower https://www.aljazeera.com/news/2021/10/5/facebook-products-harm-children-stoke-divisions-whistleblower

possível. Para isso, as plataformas criam algoritmos de informação que privilegiam conteúdos polêmicos que obrigam as pessoas a reagirem.[21] Em outras palavras, "os algoritmos que maximizam o engajamento recompensam o conteúdo incendiário"[22]. Essa lógica foi rapidamente aprendida por grupos de extrema direita,[23] especialmente ao desenvolver campanhas de desinformação.[24] Os custos dessa forma de ordenar informações são múltiplos, e muitos deles são pagos por mulheres e outros grupos especialmente vulneráveis, conforme revelado pelos vazamentos do Facebook de 2021.[25]

Além do exposto, outra série de fatores também deve ser ponderada, desde o uso de conjuntos de dados tendenciosos até a falta de diversidade na indústria de tecnologia, que repercutem na criação de espaços que facilitam vários tipos de violência, intencionalmente ou não. [26]



21 Natasha Lomas. YouTube's recommender AI still a horror show, finds major crowdsourced study. TechCrunch. July 7, 2021. https://techcrunch.com/2021/07/07/youtubes-recommender-ai-still-a-horrorshow-finds-major-crowdsourced-study/

22 Karen Hao. How Facebook got addicted to spreading misinformation. MIT Technology Review. March 11, 2021 https://www.technologyreview.com/2021/03/11/1020600/facebook-responsible-ai-misinformation/

23 Souza, L. & Varón, J. (2020) Violencia política de género en Internet. Policy paper América Latina y el Caribe. Al Sur. https://www.alsur.lat/sites/default/files/2021-07/Violencia%20Pol%C3%ADtica%20de%20G%C3%A9nero%20en%20Internet%20ES.pdf

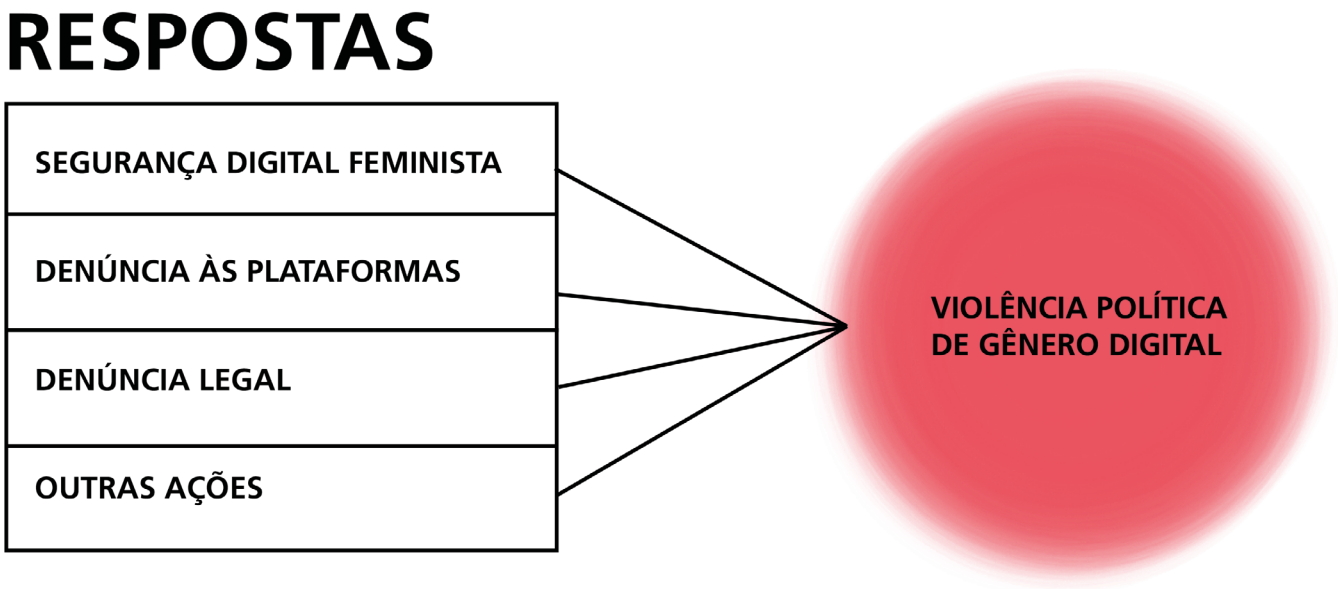
24 Samuel Woolley. We're fighting fake news AI bots by using more AI. That's a mistake. MIT Technology Review. 8 de janeiro de 2020 https://www.technologyreview.com/2020/01/08/130983/were-fighting-fake-news-ai-bots-by-using-more-ai-thats-a-mistake/

25 França24 (2021). "Facebook daña a los niños": las estruendosas revelaciones de Frances Haugen. https://www.france24.com/es/ee-uu-y-canadá/20211005-frances-haugen-facebook-senado-daños

26 A/HRC/44/57 (2020)

RESPOSTAS PARA O PROBLEMA

Como vimos, a violência política digital baseada em gênero é um fenômeno altamente complexo e multicausal, do qual mais evidências estão disponíveis recentemente. O olhar sobre o tema deve ser complexo, no qual não podem ser descartadas ações preventivas individuais, bem como ações políticas coletivas em múltiplas frentes. A seguir, é proposto um modelo de resposta que inclui o exame de quatro frentes de atuação perante a violência política de gênero online:



SEGURANÇA DIGITAL FEMINISTA

Uma resposta à violência política de gênero digital é, precisamente, a segurança digital. Esta última deve ser entendida como uma ferramenta de prevenção a ataques, bem como uma ferramenta de mitigação.

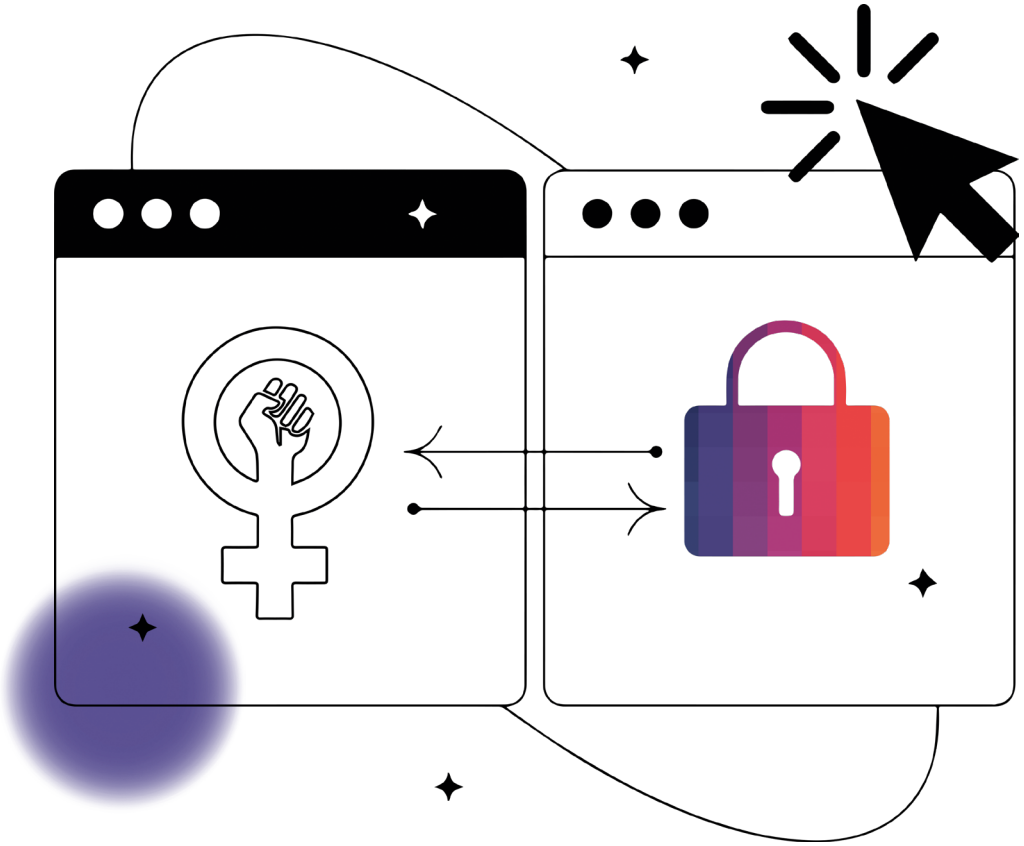
Uma visão feminista da segurança digital abandona a ideia de focar apenas na adoção de tecnologia segura e busca focar no bem-estar das pessoas por meio do cuidado digital. Isso tem diferentes implicações concretas:

- A segurança digital é entendida como o conjunto de hábitos e decisões que tomamos para prevenir e mitigar os riscos associados ao uso da tecnologia. Ou seja, mais do que tecnologias, foca nos hábitos. E mais do que buscar comportamentos universais, trata-se de defini-los localmente, de acordo com os vários riscos particulares das pessoas e de suas comunidades.
- Visa o bem-estar da pessoa, de forma integral. Ou seja, mantém-se uma perspectiva holística, onde se interligam três esferas: Segurança física Bem-estar mental e autocuidado Segurança digital.
- Ao contrário das abordagens individualistas, é também um exercício coletivo, onde, em comunidade, as pessoas se fortalecem.
- A abordagem feminista integra como mulheres, corpos e identidades, que não são governados pela cis-heteronormatividade, experimentam riscos específicos e mais ameaças por meio das tecnologias.

Modelo feminista para avaliar riscos de segurança digital

Um modelo de risco é uma ferramenta que permite medir e avaliar as ameaças enfrentadas no ambiente digital e, assim, determinar o tipo de proteção holística necessária para cuidar de suas informações, da sua organização, bem como alcançar o bem-estar individual e coletivo.

É preciso lembrar que a segurança digital também faz parte de um modelo maior, onde



a segurança física (os ataques também podem se manifestar física e materialmente) e o bem-estar psicossocial (os efeitos da violência são reais nas pessoas, em múltiplas dimensões) devem acompanhar qualquer modelo de segurança digital.

É importante fazer este exercício porque é a única maneira de identificar proativamente as ameaças que queremos priorizar, atualizar nossos hábitos de segurança e evitar riscos, reduzindo a perda de dados e o estresse associado. Mas também é um exercício importante que pode ser feito coletivamente em comunidades relacionadas, pois proporciona coordenação e solidariedade.

Um modelo feminista de avaliação de risco requer tempo e um compromisso organizacional significativo; na verdade, existem organizações e profissionais especializados que podem ajudar pessoas em risco particular.[27] Em suma, o modelo que apresentamos a seguir é um modelo simplificado, que visa demonstrar que, mais do que se concentrar na adoção de ferramentas técnicas complicadas, é necessário rever nossos hábitos diários de segurança digital, que muitas vezes são muito mais simples e próximos às pessoas.

A tabela na página seguinte mostra cinco etapas com reflexões que você precisa fazer para priorizar as ameaças[28] e suas respectivas respostas. Não há respostas corretas universais. Na tabela, também, e como exemplo, é mostrada uma possível resposta de uma pessoa fictícia que se concentra apenas no Twitter.

27 Por exemplo, o Digital Defenders Partnership ou Front Line Defenders.

28 Lembre-se: incidentes são ataques que já ocorreram e ameaças são ataques que podem ocorrer no futuro.

Este modelo dará origem a uma série de prioridades que terminarão com um plano de mitigação. Se o risco e o impacto da ameaça forem altos, as medidas de segurança digital devem ser tomadas preferencial e imediatamente. Assim, cada pessoa e organização deve ordenar suas prioridades de acordo, novamente, com seu tempo, recursos e interesses.

Com esse mapeamento inicial e priorização de ameaças, pode ser feito um plano de prevenção e mitigação para melhorar a segurança digital. As estratégias de segurança digital que focamos neste documento são duas:

- Estratégias de prevenção de riscos. Em outras palavras, uma vez identificados os riscos reais que as pessoas enfrentam na internet devido às suas atividades políticas, ações são implementadas para evitar as piores consequências desses ataques. Essa abordagem se concentra nas ameaças.
- Estratégias de mitigação. Referem-se às ações que podem ser tomadas quando ocorreu ou está ocorrendo um ataque na Internet, ou seja, essa abordagem foca nos incidentes. Para prevenir novos incidentes, precisamos detectar ameaças e, portanto, desenvolver uma estratégia de prevenção de riscos.

As ações de prevenção e mitigação podem ser caras (significa, por exemplo, a compra de um serviço ou produto) ou podem levar tempo, pois envolvem treinamento de pessoas. É importante que isso seja levado em consideração, pois pode permitir que sua comunidade ou organização faça um plano de curto, médio e longo prazo, com base nos pontos fortes e capacidades que já possuem.

Este modelo dará origem a uma série de prioridades que terminarão com um plano de mitigação. Se o risco e o impacto da ameaça forem altos, as medidas de segurança digital devem ser tomadas preferencial e imediatamente. Assim, cada pessoa e organização deve ordenar suas prioridades de acordo, novamente, com seu tempo, recursos e interesses.

Com esse mapeamento inicial e priorização de ameaças, pode ser feito um plano de prevenção e mitigação para melhorar a segurança digital. As estratégias de segurança digital que focamos neste documento são duas:

- **Estratégias de prevenção de riscos.** Em outras palavras, uma vez identificados os riscos reais que as pessoas enfrentam na internet devido às suas atividades políticas, ações são implementadas para evitar as piores consequências desses ataques. Essa abordagem se concentra nas ameaças.
- **Estratégias de mitigação.** Referem-se às ações que podem ser tomadas quando ocorreu ou está ocorrendo um ataque na Internet, ou seja, essa abordagem foca nos incidentes. Para prevenir novos incidentes, precisamos detectar ameaças e, portanto, desenvolver uma estratégia de prevenção de riscos.

As ações de prevenção e mitigação podem ser caras (significa, por exemplo, a compra de um serviço ou produto) ou podem levar tempo, pois envolvem treinamento de pessoas. É importante que isso seja levado em consideração, pois pode permitir que sua comunidade ou organização faça um plano de curto, médio e longo prazo, com base nos pontos fortes e capacidades que já possuem.

1	2	3	4	5
Identifique os ativos que deseja proteger	**Identifique adversários (de quem você deseja proteger seus ativos) e suas capacidades**	**Identifique as ameaças**	**Meça o risco**	**Determine o impacto**
Ativos: informações que colocariam em risco seu trabalho, sua organização, sua comunidade, seu bem-estar.	Pessoas, organizações ou comunidades que podem tentar atacar você. Suas capacidades (baixa, média ou alta) incluem seus recursos econômicos, sociais e tecnológicos. Lembre-se, adversários e adversárias podem ser pessoas, organizações e estados. Podem ser também pessoas muito próximos.	Ataques, incidentes ou qualquer evento que adversários e adversárias possam realizar. **Lembre-se de considerar que as interseccionalidades (gênero, raça, classe social etc.) de uma pessoa podem colocá-la em risco especial.**	Identifique a probabilidade dessa ameaça ocorrer e se tornar realidade. Sendo 1 (muito baixo) e 5 (muito alto).	Qual seria o impacto na pessoa ou organização se a ameaça se tornasse realidade (onde 1 é baixa gravidade e 5 é alta gravidade)
No Twitter: • É meu principal meio de comunicação política; quase não uso minha conta, muitas informações importantes estão lá. • Envio mensagens diretas que são privadas. • Tenho uma lista privada de pessoas voluntárias que trabalham na minha campanha e não gostaria de perdê-la	No Twitter: • Trolls comuns que querem me desacreditar; de baixa sofisticação porque só respondem a tudo o que digo. • Pessoas de outras campanhas políticas, pagos; podem ser altamente sofisticadas, suspeito que sejam organizados.	Assediar-me online com discurso anti-feminista. Já vivencio isso.	5	2
		Iniciar campanhas de desinformação com bots; isso porque já começou a acontecer com companheiras, que reduziram suas publicações.	2	4
		Apoderar-se de minhas senhas e assumir o controle da minha conta e minhas informações: recebo e-mails informando que alguém está tentando acessar minha conta.	4	5

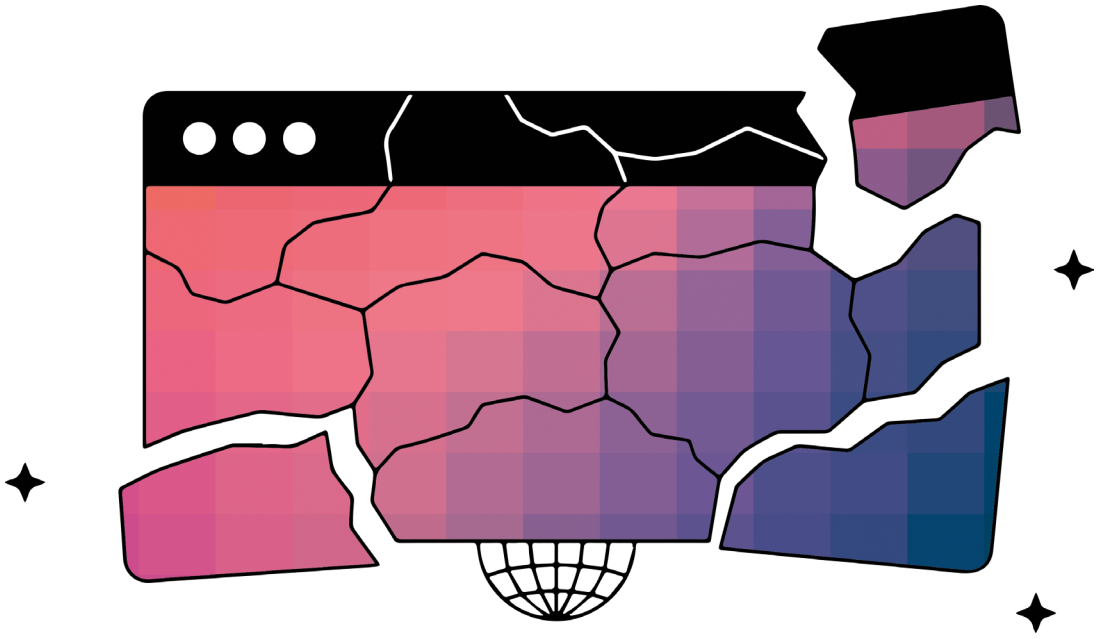
Lembre-se que todas nós já realizamos várias formas de segurança digital, ninguém começa do zero: a partir dessas práticas que já conhecemos, podem ser construídos hábitos que fortalecem nossa segurança e bem-estar individual e coletivo.

Comportamentos e ferramentas de segurança digital

Embora cada uma das ações que podem ser tomadas e ferramentas que podem ser adotadas dependam do modelo de risco, esta seção se concentra em comportamentos mínimos e ferramentas que são bastante comuns, baseadas na tabela da tipologia de ataques frequentes que analisamos anteriormente.

Isso não implica, em qualquer caso, que sejam as únicas ações que devem ser tomadas: a conversa coletiva e a transferência de experiências e boas práticas, em todos os níveis, ajudam a ter melhores estratégias de prevenção.

Para saber especificamente sobre as várias ações de segurança digital que podem atender às suas necessidades, consulte a SEGUNDA PARTE deste guia.



TIPOLOGIA DE ATAQUES	ALGUMAS AÇÕES QUE PODEM SER TOMADAS NO CONTEXTO DAS ESTRATÉGIAS DE PREVENÇÃO DA SEGURANÇA DIGITAL
Desinformação	• Verificar as contas de redes sociais • Documentar ataques e definir de padrões • Denunciar às plataformas • Verificar as informações que são compartilhadas • Pensar estrategicamente antes de discutir com bots • Excluir massivamente posts antigos de suas redes sociais • Excluir ou desativar contas que não usa mais • Compartimentar contas de redes sociais e de mensagens
Violações de privacidade	• Verificar as contas de redes sociais • Usar senhas fortes • Evitar o "phishing" • Usar gerenciadores de senhas • Denunciar às plataformas • Usar autenticação em duas etapas • Gerenciar sua identidade digital • Usar comunicações criptografadas • Compartimentar contas de redes sociais e de mensagens • Usar as configuração de privacidade nas plataformas que você usa, especialmente redes • Usar códigos de acesso em seus dispositivos
Ofensas	• Bloquear invasores da Internet • Usar as configuração de privacidade nas plataformas que você usa, especialmente redes • Denunciar às plataformas • Gerenciar sua identidade digital • Compartimentar contas de redes sociais e de mensagens
Ameaças	• Bloquear invasores da Internet • Usar as configuração de privacidade nas plataformas que você usa, especialmente redes • Denunciar às plataformas • Gerenciar sua identidade digital • Compartimentar contas de redes sociais e de mensagens
Censura	• Ser estratégica com seus posts • Documentar ataques e definir de padrões • Denunciar às plataformas • Fazer backups das informações • Compartimentar contas de redes sociais e de mensagens
Invasões	• Evitar o "phishing" • Impedir o "zoombombing" • Verificação em duas etapas • Usar senhas fortes • Fazer backups das informações • Usar autenticação em duas etapas • Usar comunicações criptografadas • Compartimentar contas de redes sociais e de mensagens • Atualizar os softwares

A importância de documentar ataques

Quanto você sabe sobre a organização por trás dos ataques que recebe pessoalmente no mundo digital? Você sabe se existem outras companheiras que estão passando pela mesma situação? Existem padrões semelhantes? Você fez alguma análise que permita entender o problema?

Documentar os ataques é importante porque nos permite analisar e buscar padrões, entender o que nos acontece como pessoas na política, mas também, se for feito como um exercício coletivo, entender o panorama que enfrentamos juntas. Além disso, também pode ser uma forma de documentar evidências que possam ajudá-la em processos judiciais.[29]

O projeto #DigitalSecurity oferece recomendações concretas sobre como iniciar esse registro de incidentes, incluindo uma proposta de planilha que você pode modificar de acordo com sua situação.[30] Nesse contexto, o projeto Acoso.Online fez um guia para documentar ataques de violência de gênero online que inclui medidas de segurança digital, que vale a pena consultar, especialmente se as informações dessa documentação forem sensíveis.[31] "Derechos Digitales" [32] também tem mais documentação nessa linha.

Bem-estar psicossocial

A abordagem psicossocial enfatiza os impactos gerados pela violência de gênero na esfera digital em diferentes níveis de vida: individual, familiar, coletivo e social. A possibilidade de recuperação, então, depende dos recursos que a pessoa tem ao seu redor, como apoio psicológico e coletivo, apoio emocional e desenvolvimento de ferramentas de proteção digital.

Nessa linha, muitas ativistas feministas no contexto latino-americano têm desenvolvido mecanismos de enfrentamento à violência online como espaços de acompanhamento feminista que buscam evidenciar a prática política do cuidado entre as mulheres.[33]

Assim, segundo organizações como a Hiperderecho do Peru,[34] há pelo menos quatro passos para incluir o bem-estar psicossocial das vítimas:

- Construir redes de apoio para garantir cuidados e uma resposta organizada. Procurar apoio psicológico se a pessoa se sentir sobrecarregada, cansada ou angustiada.
- Realizar práticas estratégicas de autocuidado e descanso das mídias digitais.
- Buscar uma fonte de motivação para empreender mudanças na segurança digital, desde a construção de plataformas diferentes das que hoje imperam a partir de paradigmas patriarcais e racistas, até não aceitar que a Internet se torne um espaço apenas de violência.

DENÚNCIA ÀS PLATAFORMAS

Como visto neste relatório, as plataformas digitais desempenham um papel particular em casos de violência política baseada em gênero: elas são as intermediárias. Nesta seção, além da responsabilidade legal que elas têm ou não, focamos nas ferramentas que muitas delas disponibilizam para mitigar esse tipo de ataque.

29 Isso dependerá dos padrões de prova digital de cada país

30 #SeguridadDigital (2028). ¿Por qué y cómo registrar y documentar incidentes? https://segudigital.org/por-que-y-como-registrar-y-documentar-incidentes/

31 Veja https://acoso.online/wp-content/uploads/2020/09/documentacion-difusion-de-imagenes.pdf

32 Veja https://twitter.com/derechosdigital/status/1443667020529213452?s=20

33 Workshop de Comunicação Feminina (2020) DIAGNÓSTICO DA VIOLÊNCIA DE GÊNERO DIGITAL NO EQUADOR. https://www.navegandolibres.org/images/navegando/Diagnostico_navegando_libres_f.pdf

34 Salas, D., Albornoz, D., Huaranga, E. (2020) Kit de cibercuidado para activistas. Seguridad digital para cuidar nuestro activismo y reapropiarnos de Internet. Hiperderecho. https://hiperderecho.org/wp-content/uploads/2020/11/Kit-de-cibercuidado-para-activistas-.pdf

Devido ao fato de muitos dos problemas das plataformas com violência de gênero terem a ver com problemas estruturais que começam desde a sua concepção, o seu modelo de negócio e até as equipes que as desenvolvem, estas ferramentas são insuficientes e estão longe de se ajustarem à realidade de países que não estão no Norte Global. No entanto, é importante saber que pode haver ferramentas que podem ajudar.

Os conteúdos mais punidos nas redes sociais

Nas plataformas existem canais para denúncia de conteúdos e interações que violem seus Termos e Condições (também conhecidos como suas Políticas da Comunidade). Para saber se determinados comportamentos das pessoas usuárias podem ser denunciadas, é importante ler as regras e, com certeza, haverá explicações sobre como denunciá-las.

No contexto deste guia, é importante destacar o "Centro de Segurança da Mulher"[35] habilitado pelas plataformas que fazem parte do mesmo conglomerado - Facebook, Instagram, WhatsApp e Messenger - com informações sobre políticas, ferramentas e outros recursos para mulheres que possam ser assediadas nelas. Da mesma forma, o Facebook, a ONU Mulheres e o Instituto Nacional Eleitoral (INE) do México lançaram dois guias com conselhos para que as mulheres na política, incluindo as candidatas, tenham mais opções para prevenir e denunciar atos de violência política com base no gênero nas redes sociais e conectar-se com suas comunidades no Facebook[36] e Instagram. [37]Mas, em geral, nas plataformas mais populares, há uma certa transversalidade em que os comportamentos são penalizados:[38]

Roubo de identidade	Facebook
	Instagram
	Twitter
Informação falsa	Instagram
Discurso de ódio	Twitter
Violação de direitos autorais	Instagram
	Facebook
	Twitter
Difamação	Facebook
"Nudes" (fotos com nudez)	Instagram
	Facebook
Phishing	Instagram
	Facebook
	Twitter
Outras violações de sua privacidade (doxing, etc.)	Facebook
	Twitter
Assédio ou outras ameaças	Instagram
	Facebook
Divulgação não consensual de imagens íntimas	Instagram
	Facebook
	Twitter

Existem outros comportamentos que depen-

35 Veja o Centro de Segurança da Mulher https://es-la.facebook.com/safety/womenssafety/tools

36 Veja Dicas da ferramenta de segurança do Facebook para mulheres líderes. #SheLeads CUANDO LAS MUJERES LIDERAN, TODOS PROGRESAN https://www2.unwomen.org/-/media/field%20office%20mexico/documentos/noticias/2021/04/%20sheleads_guide_online_es_la_foreword.pdf?la=es&vs=2947

37 Veja o GUIA DE SEGURANÇA DO INSTAGRAM PARA MULHERES NA POLÍTICA https://www2.unwomen.org/-/media/field%20office%20mexico/documentos/noticias/2021/04/mx-safety-security-guide-for-women-in-politics.pdf?la=es&vs=2843

38 Este gráfico é apenas uma amostra. As regras das plataformas estão em constante mudança e isso pode variar, mesmo entre países, por isso devem ser consultadas.

dem de cada plataforma, principalmente em questões mais complicadas como discurso de ódio e "fake news" e campanhas de desinformação. No entanto, por parte de algumas plataformas, tem havido algum compromisso público de fornecer melhores ferramentas de segurança em caso de violência de gênero.[39]

Precauções importantes

É importante repetir para não criar falsas ilusões: as soluções não são perfeitas. Especialmente quando estamos enfrentando ataques mais sofisticados.

Pode ser que as ferramentas sejam confusas de usar e não forneçam informações básicas sobre quanto tempo levará para responder.

Tenha cuidado ao solicitar a exclusão de material das plataformas, pois se você entrar com uma ação judicial posteriormente, não terá acesso a essa evidência. É sempre melhor manter um backup.

DENÚNCIA LEGAL

A seguir, apresentamos algumas iniciativas legais sobre violência política na América Latina que se dedicam especialmente à esfera digital ou fazem menção especial aos espaços eletrônicos. Isso não impede que outros projetos e leis sobre violência política de gênero sejam aplicados na esfera digital. No entanto, uma análise mais detalhada de sua eficácia e abrangência deve ser feita em estudos futuros.

Da mesma forma, os próprios ataques podem constituir outros crimes locais, como roubo de identidade ou hacking, entre muitos outros, por isso é importante consultar um especialista que analise cada caso.

É importante lembrar que, assim como outras formas de violência de gênero, além de buscar marcos regulatórios, devemos estar atentos à forma como o sistema judiciário responde a essas novas leis. Nesse sentido, e porque as leis de violência de gênero digital ainda são incipientes no continente, a evidência de seus resultados ainda é precoce. No entanto, um estudo realizado por Luchadoras no México é preocupante: apesar de desde 2012 terem sido introduzidas reformas legais em todo o país para penalizar a divulgação não consensual de imagens íntimas (uma forma muito comum de violência digital de gênero), em maio de 2020, apenas 24 processos criminais haviam sido iniciados nos poderes judiciários de sete estados do país. Além disso, apenas uma condenação havia sido emitida no Estado de Chihuahua pelo crime de "sexting" (artigo 180 bis) e três sentenças em Tamaulipas pelo crime de "Pornografia de menores e incapazes" (artigo 194 bis). [40]

OUTRAS AÇÕES

Segundo a organização equatoriana "Taller de Comunicación Mujer", é necessário "abrir espaços de diálogo dentro das organizações e entre organizações para falar sobre questões de proteção e segurança digital. O objetivo é nomear, reconhecer, analisar e socializar essa violência para desenvolver estratégias e tomar medidas de enfrentamento que permitam o empoderamento com as tecnologias."[41]

39 Hern, A. (2021) Social network giants pledge to tackle abuse of women online. The Guardian. https://www.theguardian.com/society/2021/jul/01/social-networks-facebook-google-twitter-tiktok-pledge-to-tackle-abuse-of-women-online

40 Aguirre, I., Barrera, L., Zamora, A. & Rangel, Y. (2020) Justicia en trámite. El limbo de las investigaciones sobre violencia digital en México. Luchadoras. https://luchadoras.mx/wp-content/uploads/2020/11/Luchadoras_JusticiaEnTramite.pdf

41 Taller de Comunicación Mujer (2020) DIAGNÓSTICO DE VIOLENCIA DE GÉNERO DIGITAL EN ECUADOR. Página 83. https://www.navegandolibres.org/images/navegando/Diagnostico_navegando_libres_f.pdf

PAÍS	TIPO	ESPECIFICAÇÃO
COLÔMBIA	Projeto de lei: "Por meio do qual são estabelecidas medidas para prevenir e erradicar a violência contra a mulher na vida política e outras disposições são decretadas."	"Da mesma forma, adotará medidas adequadas para promover o uso responsável e respeitoso da comunicação, por meio das novas tecnologias de informação e comunicação, em relação aos direitos das mulheres e sua participação política, nos períodos legais da campanha eleitoral."
PERU	Lei nº 31.155 que previne e pune o assédio contra a mulher na vida política	Artigo 3. Definição de assédio contra as mulheres na vida política É toda conduta exercida contra uma ou mais mulheres em razão de sua condição como tal, praticada por pessoa física ou jurídica, individual ou coletivamente, diretamente, por meio de terceiros ou utilizando qualquer meio de comunicação ou redes sociais e que tenha por objetivo prejudicar, discriminar, anular, impedir, limitar, dificultar ou restringir o reconhecimento, gozo ou exercício de seus direitos políticos. Artigo 4. Manifestações de assédio político contra as mulheres e) Divulgar imagens ou mensagens pelos meios de comunicação ou redes sociais que transmitam e/ou reproduzam relações de desigualdade e discriminação contra as mulheres com o objetivo de prejudicar sua imagem pública e/ou limitar seus direitos políticos.
PANAMÁ	Lei 184 da violência política. De 25 de novembro de 2016	Artigo 9. O Instituto Nacional da Mulher, através do Comitê Nacional contra a Violência contra a Mulher, no âmbito de suas funções, com o assessoramento da Associação de Parlamentares e Ex-parlamentares da República do Panamá, o Fórum Nacional de Mulheres de Partidos Políticos e associações ou organizações ligadas à violência política contra a mulher, em coordenação com as entidades competentes, adotarão as seguintes medidas: 6. Promover que a mídia e as redes sociais não violem os direitos e a imagem das mulheres que participam da vida pública e sua privacidade, bem como combater conteúdos que reforcem, justifiquem ou tolerem a violência política contra as mulheres.

PAÍS	TIPO	ESPECIFICAÇÃO
MÉXICO	DECRETO que altera e acrescenta vários dispositivos da Lei Geral do Acesso das Mulheres a uma Vida Livre de Violência, da Lei Geral das Instituições e Procedimentos Eleitorais, da Lei Geral do Sistema de Meios de Impugnação em Matéria Eleitoral, da Lei Geral de Partidos Políticos, da Lei Geral de Crimes Eleitorais, da Lei Orgânica da Procuradoria Geral da República, da Lei Orgânica do Poder Judiciário da Federação e da Lei Geral das Responsabilidades Administrativas.	X. Divulgar imagens, mensagens ou informações particulares de uma mulher candidata ou em exercício, por qualquer meio físico ou virtual, com a finalidade de desacreditá-la, difamá-la, desaboná-la e questionar sua capacidade ou habilidades para a política, com base em estereótipos de gênero;

Nesse sentido, além das respostas que as plataformas têm e o que a legislação propõe, são analisadas a seguir algumas iniciativas que, a partir de outros mecanismos de advocacia, buscam denunciar, conter e reverter a violência política digital de gênero.

Campanhas públicas

Essas ações de comunicação organizadas são instâncias muito interessantes para atingir públicos maiores e conscientizar sobre a violência política de gênero online. Por exemplo, no Chile, e em relação às evidências sobre o fenômeno no contexto da Convenção Constitucional, em 2020 foi lançada a campanha #DaleUnfollow contra a violência política digital de gênero.[42] Enquanto isso, no México, as Luchadoras se uniram ao Instagram para realizar uma campanha nessa plataforma para aumentar a conscientização sobre o fenômeno.[43]

Globalmente, em 2016, o Instituto Democrático Nacional para Assuntos Internacionais (NDI) lançou a campanha #NotTheCost, um apelo global à ação para aumentar a conscientização sobre o fim da violência contra as mulheres na política. O título da campanha reflete o fato de que muitas mulheres são informadas de que assédio, ameaças, abuso psicológico (pessoal e online) e agressões físicas e sexuais são "o custo de fazer política". A campanha teve uma versão no México em 2017.[44]

Observatórios independentes

A criação e coordenação de espaços independentes que acompanhem de perto o fe-

42 Observatorio Género y Equidad (2021). "#DaleUnfollow": A Articulação Territorial Feminista Elena Caffarena realiza uma campanha virtual para derrubar a violência política de gênero na Convenção https://www.humanas.cl/daleunfollow-la-articulacion-territorial-feminista-elena-caffarena-realiza-campana-virtual-para-derribar-la-violencia-politica-de-genero-en-la-convencion/

43 Veja https://www.instagram.com/p/CPGcgfALkCz/?hl=en

44 Ver https://www.ndi.org/mexico-office-launch-notthecost-noelcosto-campaign

nômeno pode não só ajudar a documentar evidências, mas também apoiar as pessoas que estão sob ataque, além de realizar diversas ações de influência política em relação à violência política de gênero na linha.

Por exemplo, no Brasil, diversas organizações da sociedade civil que trabalham com temas como cidadania e democracia, direitos digitais, feminismo interseccional, entre outros, criaram a plataforma TretAqui.org, que coleta denúncias de candidatos e candidatas que agridem e são agredidos com discurso de ódio e desinformação na Internet. Assim, em 2018, enviaram essas denúncias à Organização dos Estados Americanos (OEA), organização internacional que acompanhava de perto essas eleições.

Esses observatórios também podem abrigar ações de apoio e solidariedade diante de ataques, bem como encaminhar a espaços de apoio em segurança digital feminista.

Coalizões em partidos políticos

É importante trabalhar em códigos de conduta dentro dos partidos que incluam a violência política digital baseada em gênero; mas, como afirma o consórcio de organizações de direitos digitais da América Latina, Al Sur, em seu relatório sobre o fenômeno, é importante "manter uma abordagem suprapartidária: a mobilização deve envolver diferentes partidos políticos, pois as coalizões são essenciais para a eficácia e sustentabilidade das medidas".[45]

No entanto, é uma tarefa complicada devido aos obstáculos históricos nos partidos políticos patriarcais. Nesse sentido, talvez seja importante, em primeiro lugar, trabalhar em conjunto com coalizões suprapartidárias com militantes feministas que, juntas, possam pressionar seus próprios partidos.

Criar códigos de conduta digitais em espaços políticos que vão além do partidos

A violência política de gênero digital é muito mais ampla do que a política partidária. Portanto, é importante que esse tipo de agressão seja sancionada nos diversos códigos de conduta e ética nas instâncias políticas formais locais, regionais, nacionais e internacionais. Um exemplo recente disso é o "Código de Ética" da Convenção Constitucional do Chile, que também se concentra na violência política digital baseada em gênero. [46]

De qualquer forma, é importante trabalhar em códigos de conduta ou modelos de ética digital que possam ser adaptados localmente.

45 Souza, L. & Varón, J. (2020) Violencia política de género en Internet. Policy paper América LAtina y el Caribe. Al Sur. Página 20. https://www.alsur.lat/sites/default/files/2021-07/Violencia%20Pol%C3%ADtica%20de%20G%C3%A9nero%20en%20Internet%20ES.pdf

46 Veja https://www.chileconvencion.cl/wp-content/uploads/2021/09/Propuesta-reglamentaria-Comisio%C-C%81n-de-E%CC%81tica.pdf

SEGUNDA PARTE:

AÇÕES BÁSICAS DE SEGURANÇA DIGITAL

Esta segunda parte do guia é dedicada a especificar as várias ações de segurança digital que você pode seguir diante dos ataques mais comuns no contexto da violência política de gênero.

É importante reiterar que eles não são os únicos, mas são os básicos que você deve sempre ter em mente no contexto desse tipo de violência.

AÇÕES BÁSICAS DE SEGURANÇA DIGITAL

Senhas fortes

As senhas são uma questão fundamental e extremamente importante para evitar ataques. Muitos dos ataques acontecem porque temos senhas universais como "12345", combinações fáceis de adivinhar (aniversário) ou, mesmo que seja uma senha muito complexa, repetimos para vários serviços, então se essa informação vazar em um único serviço ela deixa você vulnerável em outras plataformas.

Se o serviço permitir, use os seguintes princípios para criar suas senhas:

- **Grandes** - Quanto maior a senha, mais difícil é decifrar.
- **Complexa** - Se possível, sempre inclua letras maiúsculas, letras minúsculas, números e símbolos, como sinais de pontuação, em sua senha.
- **Impessoal** - Evite que eles se relacionem com você de maneira pessoal, de uma forma que não possa ser facilmente adivinhada.
- **Secreta -** NINGUÉM deve conhecê-la. Se você usar uma senha e outras pessoas acessarem esse serviço (por exemplo, um terceiro que gerencia suas redes sociais) NÃO repita essa senha em outro serviço.
- **Única -** nunca as repita.

Usamos muitas senhas e é difícil lembrá-las, principalmente quando queremos torná-las mais complexas. Duas dicas:

Desde que seja impessoal, selecione um conceito básico, que seja fácil de lembrar (por exemplo, a parte de uma música que ninguém sabe que você gosta) e crie suas próprias regras com ele (faça combinações ou adicione novos elementos) de acordo com os diferentes serviços que você usa.

Use gerenciadores de senhas, que ajudem você a manter as senhas de todas as suas contas em um só lugar e também a criar senhas complexas e lembrá-las. Veja mais adiante neste guia como essas ferramentas funcionam.

Muitos "hackings" em massa acontecem todos os dias e nossos e-mails, números de telefone e senhas podem vazar. Verifique se isso aconteceu em haveibeenpwned.com e tome as medidas necessárias.

Ativar a verificação (ou autenticação) em duas etapas

A autenticação em duas etapas nos permite adicionar uma segunda camada de segurança para acessar nossas contas na Internet. Muitos serviços, de aplicativos de "chat a e-mail e redes

sociais, oferecem autenticação em duas etapas.[47] Quando ativado, um código é enviado via SMS ou e-mail, que serve como uma etapa adicional segurança no processo de login.

É um fator muito importante, pois, mesmo que alguém obtenha sua senha, precisará de um segundo passo, para que não consiga acessar sua conta e, portanto, não poderá roubar suas informações, se passar por você, etc. Agora, os hackers sabem que isso é uma possibilidade, então eles vão tentar enganá-la para lhes dar essa informação (veja a seção sobre phishing neste guia).

Habilite a autenticação de duas etapas, especialmente nas redes sociais da campanha!

Certifique-se de que o número de telefone que recebe essas mensagens de autenticação seja de uma pessoa com práticas de atendimento digital e, ao habilitar esse recurso, não se esqueça de descobrir como emitir um código de backup e mantê-lo em local secreto e seguro. Dessa forma, se você perder seu telefone, também poderá acessar sua conta com esse código.

47 Gmail https://safety.google/authentication/?hl=es_419

Usar gerenciadores de senhas

São aplicativos que nos permitem salvar e gerar chaves aleatórias e seguras. O programa é capaz de escolher senhas como "mCyXRQ3p$Kdkp\CRJxjl0v" (ou seja, que um ser humano provavelmente não adivinharia) e as lembra para você, em cada serviço. Tudo o que você precisa fazer é aprender uma senha mestra para acessar o aplicativo e nada mais.

Não é obrigatório ter este tipo de serviços e dependerá das suas necessidades. Recomenda-se conhecer a ferramenta e ver se é adequada para você. No entanto, como muitos especialistas alertam, se um adversário poderoso, como o governo, tem uma pessoa na mira, um gerenciador de senhas pode não ser o método mais seguro.[48] Para saber mais sobre essas ferramentas e como elas funcionam, confira o guia Infoativismo. [49]

Usar código de acesso em seus dispositivos

Seu celular e computador têm acesso a uma grande quantidade de informações privadas, incluindo endereços, dados bancários, além de rastros sobre suas atividades ou de outras pessoas próximas a você. Perder um dispositivo sem senha deixa a porta aberta para terceiros acessarem todas essas informações pessoais.

Por esses motivos, é importante proteger o acesso ao seu dispositivo com uma senha. A melhor opção é um PIN alfanumérico de (pelo menos) seis dígitos, mas não use números que sejam facilmente vinculados a você (como o número da placa de um carro) porque, se alguém tiver informações sobre você, poderá

48 https://ssd.eff.org/es/module/creando-contrase%C3%B1as-seguras

49 https://infoactivismo.org/que-es-un-gestor-de-contrasenas-y-para-que-sirve/

decifrar sua senha. De preferência, desative o desbloqueio por reconhecimento facial ou impressões digitais porque é muito inseguro.

Fazer backup!

Para evitar a perda de dados no caso de um dispositivo ser danificado ou roubado, é essencial fazer backup regularmente em um serviço de armazenamento online ou, preferencialmente, fisicamente em um disco rígido externo que você mantenha em um local seguro. É melhor agendar essa prática, para que suas informações não fiquem desatualizadas.

Outra forma de proteger suas informações é com o uso de pastas criptografadas. Existem vários programas como Truecrypt, Sophos Free Encryption ou Axcrypt que permitem adicionar uma senha a arquivos e pastas em seu computador, para que apenas pessoas com a chave possam decifrá-los.

Prevenir phishing

Essas técnicas procuram induzi-lo a revelar senhas ou instalar malware[50] no seu dispositivo. Um ataque de phishing geralmente vem na forma de uma mensagem (via e-mail, SMS, chat, etc.) que parece legítima e tem como objetivo convencê-lo a:

- clicar em um link;
- abrir documentos;
- instalar algum software em seu dispositivo;
- ou digitar seu nome de usuário e senha em um site que parece real.

O phishing é usado tanto por criminosos comuns quanto por agentes maliciosos e Estados. É uma técnica comum e transversal, que ocorre em todas as plataformas (e-mails, chats, SMS, etc.) portanto devemos ter muito cuidado, sobretudo porque nas nossas campanhas políticas temos de estar mais alertas às informações que tratamos nos nossos dispositivos.

50 Malware é um termo geral para se referir a qualquer tipo de "software malicioso" projetado para se infiltrar no seu dispositivo sem o seu conhecimento. São ataques comuns a jornalistas, defensores e defensoras de direitos humanos e figuras políticas https://www.dw.com/es/nso-group-se%C3%B1alado-de-espiar-a-50000-tel%C3%A9fonos-con-pegasus/a-58311353

Para evitar isso, lembre-se de cinco dicas:[51]

APENAS DIGITE SENHAS EM SITES REAIS	VERIFICAR OS ENDEREÇOS DE E-MAIL DOS REMETENTES	ATIVAR A VERIFICAÇÃO EM DUAS ETAPAS	ABRIR DOCUMENTOS SUSPEITOS NO GOOGLE DRIVE	MANTER SEU SOFTWARE ATUALIZADO
Em geral, os serviços NUNCA solicitarão que você verifique sua conta, nem caso de emergência. A utilização deste tipo de mensagens maliciosas é comum porque obriga a agir rapidamente e a não pensar muito. Se a emergência parecer real, verifique diretamente com as fontes. Insira senhas apenas em sites reais que tenham o cadeado de criptografia na URL. Cuidado, eles tentarão enganá-lo e podem até usar a imagem do site original.	Os endereços correspondem ao que eu conheço? Às vezes, olhamos apenas para o nome e não para o e-mail para abri-lo. Tome um segundo para verificar, cuidado que eles tentarão enganá-lo nos mínimos detalhes, por exemplo, trocando um i por um l. Em caso de dúvida, não clique nem baixe nenhum arquivo.	A autenticação em duas etapas nos permite adicionar uma segunda camada de segurança para acessar nossas contas na Internet. Ou seja, se eles conseguirem obter sua senha, a segunda etapa de verificação poderá anular seus propósitos.	Se recebermos documentação suspeita, devemos verificá-la antes de abri-la. Nesses casos, não clique no arquivo para baixá-lo. Em vez disso, abra-o no Google Drive ou em outro leitor de documentos online. Isso converterá o documento em uma imagem ou HTML, o que quase certamente impedirá que você instale software malicioso em seu dispositivo. Depois que a legitimidade do arquivo for verificada, você poderá baixá-lo.	Os ataques de phishing usando malware, frequentemente são baseados em vulnerabilidades no software. Assim que um bug for conhecido, um fabricante de software lançará uma atualização para corrigi-lo e notificá-lo. Não procrastine. Mantenha o software atualizado em todos os seus dispositivos!

51 Para obter mais dicas para evitar phishing, consulte https://ssd.eff.org/pt-br/module/como-evitar-ataques-de-pesca-phishing

Atualizar seus softwares

A atualização de seus dispositivos é essencial para sua segurança digital, pois as empresas desenvolvedoras descobrem constantemente vulnerabilidades em seus programas, além de novas ameaças à segurança, como malware. Muitas pessoas aproveitam essas falhas para realizar ataques de informáticos.

Em resposta, os desenvolvedores lançam atualizações e patches para corrigir vulnerabilidades, portanto, você precisa manter seu sistema operacional e o software que usa atualizados. Embora não representem uma garantia infalível, as atualizações reduzem significativamente o risco de ser vítima de um ataque.

Meus dispositivos estão grampeados?

É quase impossível saber sem a intervenção de especialistas, então NÃO acredite em testes que rodam na Internet, pois muitos deles também podem ser ataques maliciosos. Por isso, é importante ativar medidas de precaução, entendendo que uma parte importante dos malwares de agentes privados ou estatais perigosos se aproveitam de vulnerabilidades dos softwares, bem como de ataques de phishing. Se tiver dúvidas fundamentadas, melhor contatar e consultar o CiviCERT (Computer Incident Response Center for Civil Society).

Usar comunicações criptografadas

A criptografia é o processo matemático de tornar uma mensagem ilegível, exceto para a pessoa que possui a chave para descriptografá-la em um formato legível. Ou seja, mesmo quando uma pessoa puder interceptá-lo, se estiver criptografada, ela o verá em um código matemático e não conseguirá entendê-la. A criptografia nas comunicações pode ocorrer em diferentes níveis em nossos diferentes canais de comunicação, e isso exigirá mais ou menos esforços de adoção, dependendo do canal.

Existem várias maneiras de adotar a criptografia em nossas comunicações, como usar VPN ao usar WiFi público,[52] usar https em nosso site e nos que visitamos,[53] ou aprender a criptografar nossos e-mails,[54] entre outras ações.

Mas devido à natureza massiva de seu uso, é importante optar por um serviço de mensagens criptografadas que possa ser fundamental para, pelo menos, as comunicações políticas que você possui. Os níveis de segurança das plataformas variam sempre de acordo com diferentes fatores, por isso é importante estar sempre informada. De qualquer forma, apresentamos a você informações básicas sobre os serviços de chat que podem orientá-la em suas decisões de comunicação.

52 Veja https://www.adslzone.net/reportajes/internet/mejores-vpn-gratis/

53 Consulte https://es.wikipedia.org/wiki/HTTPS_Everywhere

54 Veja https://ayudaleyprotecciondatos.es/2021/07/10/cifrar-correo-electronico/

				
Signal	**WhatsApp**	**Telegram**	**Wire**	**Facebook Messenger**
É uma solução multifuncional gratuita de mensagens, chamadas de voz e mensagens em grupo que usa sua própria criptografia de ponta a ponta. O protocolo de criptografia do Signal é tão forte que o WhatsApp e o Facebook Messenger também o utilizam. Mas ao contrário do Facebook, a empresa matriz da Signal é uma fundação sem fins lucrativos.	Usa o protocolo de criptografia do Signal de ponta a ponta em todas as mensagens desde 2016 e adicionou continuamente ajustes aos recursos de segurança e privacidade do aplicativo, como convites e controles de grupo rígidos para que a pessoa que o usa esteja sempre ciente de quem está lendo seu grupo. O WhatsApp agora é propriedade do Facebook, alguns dados comportamentais de quem tem uma conta do WhatsApp agora são compartilhados com o Facebook, mas as mensagens permanecem completamente isoladas.	Ao contrário de outros aplicativos de mensagens criptografadas, a criptografia de ponta a ponta não é habilitada por padrão no Telegram. Para obtê-la, você deve optar por um modo de bate-papo secreto.	Possui criptografia de ponta a ponta para mensagens instantâneas, chamadas de voz e vídeo. Usa seu próprio protocolo de criptografia baseado no protocolo Signal, e seu código é de fonte aberta e sujeito a auditorias externas de segurança. As versões móveis e web do aplicativo são gratuitas, com nível premium disponível para empresas.	As versões móveis do aplicativo incluem opções de comunicação criptografada de ponta a ponta na forma de conversas secretas. Com base no mesmo sistema de criptografia usado no Signal, as conversas secretas exigem que os usuários optem pelo recurso. Você ainda está vulnerável a capturas de tela, e as limitações de assinatura e de dispositivo único podem ser um problema. Além disso, pertence ao Facebook.

Para qualquer canal de comunicação que você usar, lembre-se de desabilitar a visualização da mensagem na tela inicial do seu dispositivo móvel. Uma pessoa desconhecida pode ver facilmente informações importantes.

AÇÕES DE SEGURANÇA DIGITAL EM REDES SOCIAIS

As redes sociais são, reconhecidamente, um dos espaços onde mais se recebe violência política de gênero na Internet. Portanto, além da camada básica de segurança digital que vimos na seção anterior, é importante adicionar outras ferramentas e comportamentos específicos.

GERENCIAR SUA IDENTIDADE DIGITAL

Uma parte importante da nossa vida pessoal, social e política acontece em plataformas digitais que são disponibilizadas por empresas privadas, por isso fazem parte de uma estratégia de obtenção de lucros. Como vimos na primeira seção deste guia, uma parte importante dessas plataformas se baseia no modelo de negócios de oferecer serviços gratuitos em troca da coleta de dados pessoais das pessoas, por isso muitas de suas lógicas buscam persuadir as pessoas a compartilhar todo tipo de pensamentos e relações.

Isso inclui as configurações de privacidade de dados que vêm por padrão nas redes sociais e são sempre mínimas.

Nesse contexto, são expostas nossas vidas pessoais, sociais e políticas. Isso significa que é importante ter clareza sobre a extensão do uso de nossa identidade digital e gerenciá-la de acordo com nossos objetivos e, também, nosso modelo de risco.

Gerenciar nossa identidade digital significa ter o maior controle possível sobre quais dados pessoais (meus e dos que me cercam) quero que sejam publicados na Internet. Isso é particularmente importante para as mulheres na política, já que muitos ataques hoje são recebidos com base em dados pessoais que os agressores manipulam.

Para isso, recomendamos algumas ações que podem ser úteis:

Verificar as contas de redes sociais

Este é um serviço oferecido pelas redes sociais para poder autenticar contas e verificar se quem diz ser o dono da conta de fato o é. Cada plataforma fornece um selo de conta pública verificada, que ajuda o público a ter informações concretas sobre a fonte e, para quem possui conta, para evitar roubo de identidade ou confusão com contas semelhantes, como paródias.

Ainda assim, algumas ressalvas:

- Contas verificadas podem representar um risco de segurança, chamando a atenção de hackers que podem tentar assumir o controle de uma conta verificada para comercializar o perfil com base no selo e número de seguidores.
- Em geral, não é possível transferir uma conta verificada para outra. As contas verificadas não podem alterar o nome da conta nem transferir essa verificação para uma conta diferente. Já que o objetivo do selo de verificação é que as pessoas saibam que a conta foi verificada.
- Não é um exercício automático e muitas vezes a verificação é negada, sem muitas explicações por parte das plataformas.
- Os serviços de mídia social atualmente populares que oferecem verificação de contas incluem: Twitter, Instagram, Facebook e YouTube.

Em sua campanha, verifique as contas oficiais de suas redes sociais! Assim, você pode ter um canal oficial de comunicação com as pessoas e reduzir o risco de roubo de identidade.

Compartimentar contas de mídia social e mensagens

Sua identidade digital não precisa ser uma só. Você pode ter vários perfis, diferentes dispositivos! Por isso é importante que você pense estrategicamente em suas comunicações, principalmente quando você tem uma atividade política. Que tipo de interações você terá? Você vai compartilhar aquela foto da sua família? As informações que estou postando podem fornecer mais pistas sobre minha localização do que eu gostaria?

Uma recomendação comum é, se você concluir do seu modelo de risco, dividir sua identidade digital em uma de natureza mais pessoal (onde você compartilha informações apenas com seu círculo mais próximo e talvez use um pseudônimo) e outra, pública, onde você compartilha com o resto das pessoas.

Fazer configuração de privacidade nas plataformas que você usa, especialmente redes sociais e mensagens

Depois de definir a maneira como você desenvolverá sua identidade digital, revise e

modifique as configurações de privacidade de sua conta, de acordo com sua estratégia. Lembre-se de que há muitas opções, desde ler apenas as pessoas que você segue, silenciar interações que você não quer ter, desligar o georreferenciamento de suas postagens (que mostra as coordenadas do local onde você está postando), limitando quem pode lhe enviar mensagens diretas, entre muitas outras que podem melhorar a sua experiência online.

Não deixe as configurações de privacidade que as redes sociais possuem por padrão, pois elas sempre serão as mínimas possíveis. Verifique-as constantemente porque, devido a alterações nos Termos e Condições, as plataformas podem alterá-las. Não tenha medo de experimentá-las: a internet não vai "quebrar" se você testar as opções e sempre poderá voltar.

Bloqueie o ódio

As redes sociais contam com mecanismos de segurança que permitem aos usuários bloquear, silenciar e denunciar os conteúdos abusivos, mas se trata de um processo que leva muito tempo posto que, requer a leitura das publicações negativas e decidir como responder ou não.[55]

Para economizar tempo e energia e evitar a perda acidental de informações importantes e comentários pertinentes, existem ferramentas como Block Party for Twitter.[56] Com Block Party você pode filtrar os tweets de acordo com uma série de critérios e salvá-los em uma pasta separada. Por exemplo, você pode manter os comentários longe de contas novas ou sem foto de perfil, que são mais propensas a serem contas falsas ou até bots criados para atrapalhar discussões ou intimidar usuários legítimos. Você pode revisar os tweets mais tarde, quando estiver mentalmente preparado, ou pode até pedir a outra pessoa para revisá-los para você.

55 Consulte https://help.twitter.com/es/safety-and-security/control-your-twitter-experience

56 Veja https://www.blockpartyapp.com

AÇÕES DE SEGURANÇA EM VIDEOCONFERÊNCIAS

Devido às restrições obrigatórias de mobilidade devido à pandemia do COVID-19, em muitos países houve um aumento maciço de reuniões virtuais por meio de plataformas eletrônicas, como Google Meet, Jitsi ou Zoom, entre outras.

Nesse contexto, um fenômeno bastante comum também se popularizou: invasões indesejadas de reuniões virtuais para capturá-las e entregar mensagens violentas, muitas delas misóginas e racistas. As atividades feministas foram particularmente afetadas. Devido à popularidade da plataforma Zoom e suas, até então, medidas de segurança precárias, esse fenômeno ficou conhecido como zoombombing.

Como as conferências e seminários públicos online são essenciais em campanhas políticas, é muito importante levar em consideração as ações de segurança ao organizá-las.

Que plataforma de videoconferência escolher?

De acordo com a organização latino-americana Derechos Digitales em seu guia especial para escolha de uma ferramenta de videochamada, não existe uma plataforma perfeita, portanto a adequação de um software dependerá em grande parte das necessidades específicas da videochamada, como: oferecer segurança contra o interceptação de chamadas, seu custo monetário, sua massividade, possibilidade de gravação, entre outros.

Para determinar qual ferramenta pode ser interessante para suas necessidades, recomendamos que você consulte o diagrama especial que a Derechos Digitales possui em seu guia.[57]

Impedir o "zoombombing"

- **Gere um ID de reunião aleatório**: evite colocar nomes na reunião porque eles podem ser facilmente descobertos, use IDs aleatórios que muitas das plataformas permitem.
- **Controle sobre pessoas convidadas:** Não compartilhe massivamente o link da reunião. Recomenda-se utilizar a função que permite proteger reuniões virtuais através de uma senha de acesso, bem como fazer uso das salas de espera em que os participantes podem estar enquanto o anfitrião prepara tecnicamente a reunião. Então, este último pode aprovar a integração das pessoas que estão na sala de espera.
- **Mantenha o controle da tela:** O host deve manter o controle do que é transmitido na tela a todo momento, caso um participante queira compartilhar conteúdo, é recomendável que ele envie previamente ao host para transmissão em uma reunião; ou que antes de abrir massivamente a reunião, dê a essa pessoa a possibilidade de compartilhar a tela.
- Se ocorrer um ataque, o host pode tirar proveito das medidas de segurança, como remover invasores da reunião, limitar o compartilhamento de tela e restringir o bate-papo.[58]

57 Veja https://www.derechosdigitales.org/wp-content/uploads/pub_videollamadas.pdf

58 Particularmente para ver as etapas de segurança na plataforma Zoom, consulte https://cudi.edu.mx/noticia/recomendaciones-de-seguridad-para-administradores-de-las-cuentas-zoom-del-servicio-vc-cudi

AÇÕES DE SEGURANÇA PARA EVITAR DESINFORMAÇÕES E FAKE NEWS

A desinformação é um dos ataques que, ultimamente, mais têm causado preocupação em relação à governança da Internet e debates sobre liberdade de expressão; ainda mais, muitos Estados a consideram como parte de ataques à sua segurança cibernética. No caso da violência política digital de gênero, a desinformação geralmente se dá por meio de campanhas de difamação contra a líder (com o objetivo de desacreditá-la) e disseminação de informações falsas (muitas vezes ligadas à sexualidade e ao casamento).

Embora seja um problema complexo, com múltiplas camadas, que ultrapassa os hábitos de segurança digital e que depende de ações das comunidades, dos Estados, mas também das plataformas, existem ações que podem nos ajudar a enfrentá-lo melhor a partir da segurança digital.

Verifique as informações que são compartilhadas

Não espalhe notícias falsas (fake News), um perfil político responsável deve ter muito cuidado com isso porque você pode receber reações muito fortes por causa disso. Aqui estão cinco maneiras de evitar desinformação nas mídias sociais e mensagens:

- Antes de compartilhar, verifique a origem: no calor do imediatismo das redes sociais ou outros meios de comunicação como chats, compartilhamos tudo, imediatamente, sem antes verificar. Nossa ação consciente e da comunidade pode acabar com a cadeia de desinformação. Se a fonte for desconhecida ou suspeita, apenas não compartilhe.
- Existem muitos sites que parecem ser legítimos, mas não atendem aos padrões mínimos de veracidade.
- Não se deixe levar por clickbait. Este último é um conceito que se refere ao conteúdo projetado intencionalmente para capturar a atenção das pessoas e levá-las a clicar nele. Em outras palavras, é uma espécie de sensacionalismo que busca captar a atenção. Essa técnica é frequentemente usada em campanhas de desinformação. Lembre-se, o título ou resumo muitas vezes está longe do conteúdo. Antes de compartilhar, leia e verifique.
- Veja a data de publicação. Algo tão simples é crucial. Muitas vezes, notícias antigas são compartilhadas maliciosamente sem informar a data, como forma de adicionar polêmica a uma discussão atual. Você tem que tirar alguns segundos e conferir a data, se não tiver, procure a notícia e veja se tem outro portal que a levou a sério e confira lá.
- Envie as notícias para verificadores de notícias falsas especializados em seu país (geralmente conhecidos como verificadores de fatos).
- Denuncie perfis falsos em redes sociais que o permitam.

Pense estrategicamente antes de discutir com bots

Está cada vez mais difícil saber se é uma conta automatizada ou semiautomática. Há, no entanto, algumas dicas para ponderar se se tratam desses perfis que são:

a) se o perfil tem data de criação recente,

b) se tem mensagens repetitivas e/ou

c) se a imagem pessoal utilizada não é perso-

nalizada ou se foi criada por Inteligência Artificial para simular uma pessoa real.[59]

No Twitter, por exemplo, você pode restringir a visualização de perfis sem verificação por telefone ou que não tenham um avatar, o que também pode buscar certos graus de anonimato para atacar.

Agora, como muitos desses perfis são feitos para fins maliciosos, você deve deixar para trás a ideia de que **pode entrar em condições de diálogo e pesar, estrategicamente, se você quer se envolver em interações com eles.** Isso porque você deve sempre lembrar que nas redes sociais "atenção" é recompensada com visibilidade, então responder ou não responder torna-se projetar quanta visibilidade você quer dar ao diálogo e espalhar a mensagem.

Uma estratégia, por exemplo, pode ser ver quanta visibilidade a fonte original da mensagem de ódio ou desinformação tem, por exemplo, através de quantas vezes a mensagem foi compartilhada. Se tiver um escopo significativo, talvez você possa planejar uma resposta. Se este for o caso, você deve estar preparado para provavelmente ter uma avalanche de respostas de apoio e rejeição. Para que isso aconteça, jogar pelas regras dos algoritmos de mídia social seria bom, porque leva sua mensagem a mais pessoas. No entanto, você pode silenciar as respostas à sua mensagem ou permitir que apenas as pessoas que você segue respondam a você, para evitar interações perigosas.

59 Veja https://www.xataka.com/robotica-e-ia/asi-puedes-superar-test-para-detectar-que-fotos-celebrities-han-sido-creadas-mediante-inteligencia-artificial

Seja estratégica com seus posts

As regras da comunidade, também conhecidas como termos de serviço, são os parâmetros que as plataformas têm para definir qual conteúdo é ou não aceitável em sua plataforma. Eles são diversos, podem variar muito entre as plataformas e muitos deles entram em conflito com a liberdade de expressão. Por exemplo, o Instagram não aceita a publicação de mamilos femininos, mas aceita de masculinos, o que também teve impacto na censura de muito ativismo feminista na plataforma. Ou no Facebook e no Twitter há evidências de que o discurso palestino é censurado.[60]

Independentemente das ações das plataformas serem legítimas ou até legais, é importante estar atento às publicações que são feitas, pois muitas podem ser denunciadas de forma maliciosa, podendo não só rebaixar a publicação como até penalizar o seu perfil. Nesse sentido, é importante pesar quais mensagens você vai entregar e, se estiver disposto a correr o risco, tomar todas as medidas pertinentes, como multiplicar os canais de comunicação de sua campanha (incluindo, esperamos, seu próprio site onde pessoas podem encontrar informações sobre seu perfil político, e que esses conteúdos não dependem das regras das redes sociais).

As regras das plataformas, além disso, mudam de tempos em tempos. Para ter um registro das últimas mudanças, você pode consultar o projeto do Centro de Estudos sobre Liberdade de Expressão e Acesso à Informação (CELE) da Universidade de Palermo, Letra Pequena. [61]

60 IFEX (2021) Facebook e Twitter devem parar imediatamente de censurar o conteúdo palestino https://ifex.org/facebook-and-twitter-must-immediately-stop-censoring-palestinian-content/

61 Veja https://letrachica.digital/

Sobre o que é considerado violência, o Facebook disponibiliza conselhos sobre do que pode ser publicado ou não em suas plataformas que vale a pena conhecer porque, em geral, podem ser aplicados em campanhas políticas.[62]

Exclua massivamente posts antigos de suas redes sociais

Se você usa redes sociais e sua linha estratégica de publicações mudou ao longo do tempo, você pode estar interessado em excluir publicações antigas. Muitas vezes, os ataques de assédio são feitos revivendo postagens feitas há muitos anos e, outras vezes, sua publicação anos depois faz parte de estratégias de desinformação mais produzidas.

A exclusão manual de postagens do Twitter é quase impossível, especialmente se você tem um perfil há anos. Para fazer isso com mais conforto, existem várias ferramentas que podem te ajudar, muitas delas são pagas.[63] No Facebook, por exemplo, você pode excluir e também restringir postagens antigas.[64]

Outra prática relacionada que você pode adotar é o hábito de deletar suas postagens nas redes sociais a cada determinado período de tempo.

Exclua ou desative contas que você não usa mais

As contas que você não usa mais podem ser uma fonte de deturpação para campanhas de desinformação ou, também, uma fonte de informação que você não deseja mais compartilhar. Exclua as contas que você não usa mais. Cuidado, pode levar tempo: redes sociais como o Facebook, por exemplo, demoram algumas semanas para excluir completamente a conta.

62 Veja https://transparency.fb.com/es-la/policies/community-standards/violence-incitement/?from=https%3A%2F%2Fwww.facebook.com%2Fcommunitystandards%2Fcredible_violence

63 Veja https://transparency.fb.com/es-la/policies/community-standards/violence-incitement/?from=https%3A%2F%2Fwww.facebook.com%2Fcommunitystandards%2Fcredible_violence

64 Veja https://www.adslzone.net/como-se-hace/facebook/borrar-publicaciones-antiguas-facebook/

MAIS RECURSOS DE AJUDA

Abaixo está uma lista de recursos mais úteis que podem ajudar os políticos e suas equipes a conhecer mais ações de segurança.

MODELO	NOME	DESCRIÇÃO
Mesas de ajuda	Vida Ativa[1]	Linha de apoio para vítimas de violência de gênero online para a América Latina.
	Acesse agora a Linha Direta de Segurança Digital[2]	Ela trabalha com pessoas e organizações em todo o mundo para mantê-las seguros online. Se você estiver em risco, eles ajudam a melhorar suas práticas de segurança digital para mantê-lo fora de perigo. Se você já está sob ataque, eles fornecem assistência de emergência de resposta rápida.
Segurança digital em manifestações	Karisma: Dicas de segurança digital: antes, durante e depois de uma manifestação[3]	Informações sobre algumas das dúvidas mais recorrentes que temos recebido de pessoas que estão exercendo seu direito de protestar nas ruas.
	Várias organizações: "¡No me cuidan!" Contra a violência institucional masculina. De 25N a 8M[4]	Este Kit Protesto Feminista tem como objetivo fornecer ferramentas para nos prepararmos e nos protegermos contra a violência institucional masculina em mobilizações.
Videoconferências	Infoativismo: Como iniciar um webinar: ferramentas para transmissão ao vivo[5]	Opções de ferramentas e um breve passo a passo.
Segurança digital em geral	Relacionado: Segurança digital: conceitos e ferramentas básicas[6]	Este guia foi escrito com enfoque em jornalistas, defensores de direitos humanos, ativistas e pessoas que, independentemente de seu espaço, de desenvolvimento profissional, querem começar no caminho da segurança e privacidade digital.
	FLIP: Manual Antiespião: ferramentas para a proteção digital de jornalistas[7]	Seu objetivo é melhorar o conhecimento e a conscientização sobre a segurança digital da informação e das comunicações.

1 Veja https://vita-activa.org/
2 Consulte https://www.accessnow.org/help/
3 Veja https://web.karisma.org.co/kit-de-seguridad-digital-para-antes-durante-y-despues-de-la-protesta/
4 Veja https://hiperderecho.org/vigilandovigilantes/assets/resources/kit-feminista.pdf
5 Veja https://infoactivismo.org/como-lanzar-un-webinar-herramientas-para-transmision-en-vivo/
6 Veja https://conexo.org/project/921/
7 Veja https://www.flip.org.co/images/Documentos/manual-antiespias.pdf

AUTORA

Paz Peña (pazpena.com) é consultora independente e ativista em tecnologia, feminismo e justiça social. Ela é co-criadora do Acoso.Online, um recurso da web que fornece informações e recomendações confiáveis para vítimas da divulgação não consensual de imagens íntimas na Internet em 19 países da América Latina, Caribe e Espanha. É jornalista, formada em Comunicação Social (Pontifícia Universidade Católica de Valparaíso, Chile) e mestre em Estudos de Gênero e Cultura (Universidade do Chile).

FICHA TÉCNICA

Fundação Friedrich Ebert no Chile

Hernando de Aguirre 1320 I Providence I
Santiago de Chile

Responsável

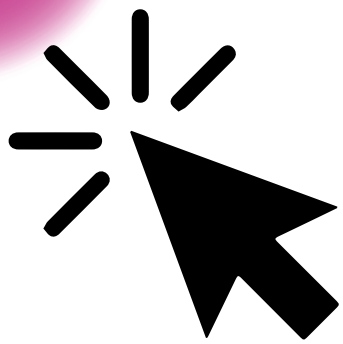
Dra. Cäcilie Schildberg
Diretora do Projeto Regional
FESminismos I Representante da FES Chile

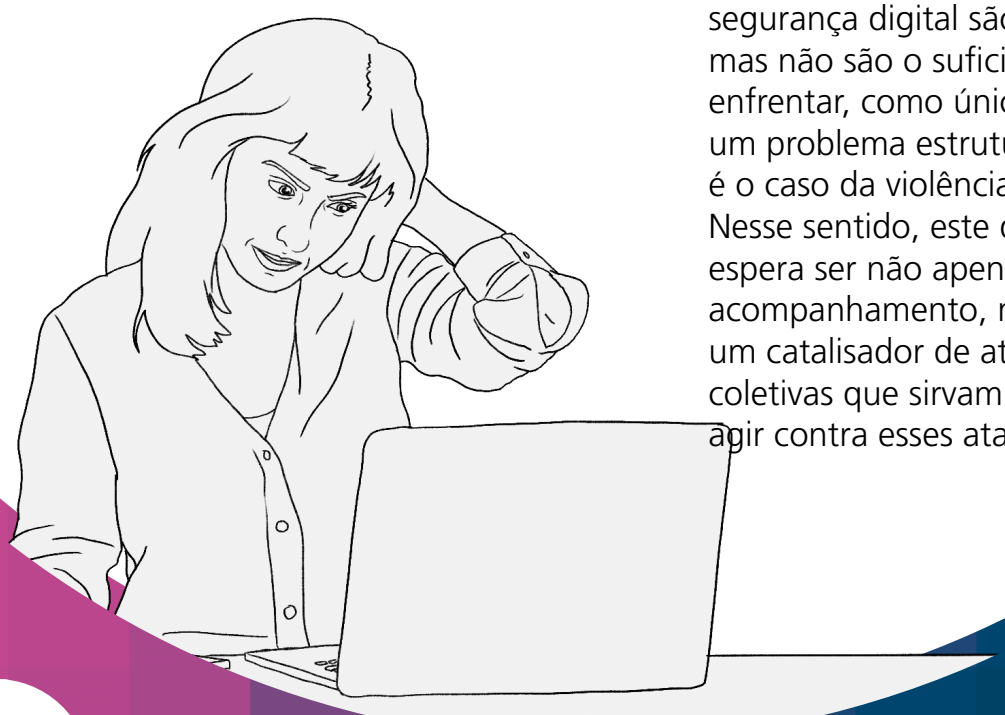
Sarah Herold
Coordenadora Regional de Projetos
FESminismos
www.fes-minismos.com
@fesminismos

Edição/correção: Matias Galleguillos Muñoz

Projeto e diagramação: María Elvira Espinosa Marinovich
Tradução: Silvia Peres

ISBN 978-65-87504-55-1





A violência política contra as mulheres compreende todo e qualquer ato ou ameaça de violência baseado em gênero, que resulta ou pode resultar em danos físicos, sexuais ou psicológicos ou sofrimento, e está dirigido contra a mulher na política por sua condição de mulher.

Este é um guia de recomendações de segurança digital e com enfoque feminista para pessoas e organizações que enfrentam violência política de gênero digital.

É um trabalho que visa enfatizar a ideia de que os hábitos de segurança digital são importantes, mas não são o suficiente para enfrentar, como único trunfo, um problema estrutural, como é o caso da violência de gênero. Nesse sentido, este documento espera ser não apenas um guia de acompanhamento, mas também um catalisador de atividades coletivas que sirvam para resistir e agir contra esses ataques.

FESMINISMOS

#TOMAPARTIDO

FRIEDRICH EBERT STIFTUNG