Instituto de Pesquisa em Direito & Tecnologia do Recife

NÃO É PARANOIA

NÃO É PARANOIA

A violência de gênero online é real





FICHA TÉCNICA

Realização:

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

Equipe:

Coordenação:

Aline Melo

Autoras:

Clarissa Mendes

Mariana Canto

Raquel Saraiva

Revisão:

Aline Melo

Projeto Gráfico:

Estúdio PUYA!

Produzida com apoio do Fundo de Populações das Nações Unidas - UNFPA, através do edital "Nas Trilhas de Cairo".

Como citar:

IP.REC - INSTITUTO DE PESQUISA EM DIREITO E TECNOLOGIA DO RECIFE. Não é Paranoia: a violência de gênero online é real. Recife: IP.rec, 2025. Disponível em: https://ip.rec.br/publicacoes/nao-e-paranoia/

APRESENTAÇÃO

Existem mais de 40 tipos de violência de gênero facilitada pela tecnologia.

Apesar desse número expressivo, identificar essas violências no ambiente online é um desafio: além da dificuldade de reconhecer os novos mecanismos e ferramentas no meio digital que são usadas para atingir meninas e mulheres, as vítimas têm seus sentimentos invalidados e, muitas vezes, não entendem que estão sendo alvos de uma ação criminosa que precisa ser denunciada.

Essa violência **não é paranoia**: e podem resultar em danos psicológicos, físicos, sexuais, sociais e políticos e outras violações dos direitos de meninas e mulheres. Impactos graves na saúde mental são as consequências mais comuns desse crime.

Esta cartilha é uma produção do **Instituto de Pesquisa em Direito e Tecnologia (IP.rec)**, com apoio do Fundo de População das Nações Unidas (UNFPA) e da Embaixada Britânica pelo edital Nas Trilhas de Cairo, para fortalecer o combate à violência de gênero online.

Neste material, você vai aprender como identificar, prevenir e denunciar crimes de **deepnudes** (falsos nudes), **stalking** (perseguição online), **discurso de ódio**, **violência política** e **doxxing** (vazamento de informações pessoais).

Por fim, esta cartilha tem a importante missão de sensibilizar a sociedade sobre as violências enfrentadas pelo gênero feminino no meio digital e ajudar a construir um espaço online seguro para que meninas e mulheres possam se expressar livremente.

DEEPNUDES

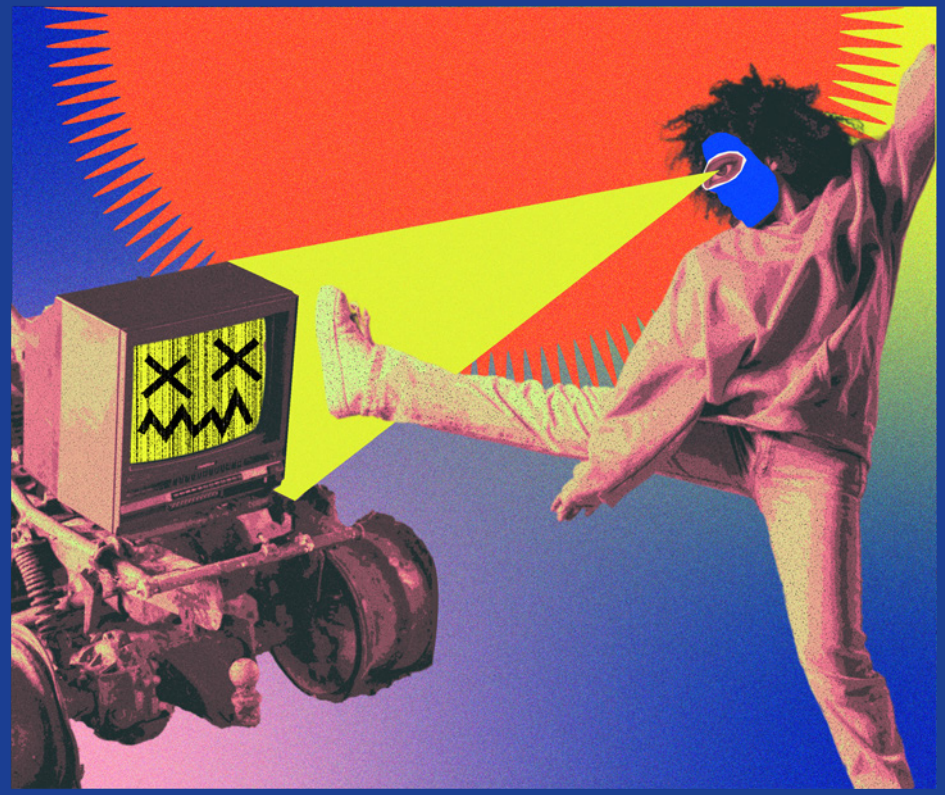
As chamadas “deepfakes” são falsificações resultantes de programas de edição de imagem, vídeo e som, gerados a partir de ferramentas de inteligência artificial, que podem ser ultra-realistas.

Já as **deepnudes** são um tipo de deepfakes que contêm imagens de nudez e se tornam problemáticas quando ocorrem de forma não-consensual, ou seja, sem o consentimento da vítima. Por isso, podem ser consideradas uma forma de violência ou abuso sexual digital.

99%

dos alvos de deepnudes são mulheres.

Referência: Flynn, A., Powell, A., & Hindes, S. (2021). Technology-facilitated abuse: A survey of support services stakeholders (Research report, 02/2021).



Ainda que as imagens sejam falsas, os efeitos são reais: as vítimas de abuso digital têm taxas elevadas de problemas de saúde física e mental, como ansiedade, depressão, automutilação e suicídio. Pode impactar nas relações com o emprego, família e vida social, além de ter um efeito inibitório sobre a liberdade de expressão das mulheres.

Identificação

Há algumas **ferramentas de detecção** para identificar imagens falsas, mas elas nem sempre acompanham o ritmo da geração de conteúdo. Alguns exemplos são o AI Image Detector, GPT Zero, Originality.AI, Mayachitra, AI or Not, Deepware Scanner, entre outros.

Além disso, os conteúdos gerados costumam apresentar algumas **falhas** que as denunciam. Orelhas, olhos e mãos são elementos que as ferramentas ainda têm dificuldade de reproduzir, mas a tendência é que esses erros se tornem a cada dia menos perceptíveis, na medida em que as ferramentas se aprimoram.

Prevenção

Não é brincadeira! Apesar das imagens de deepnudes não serem reais, seus efeitos são - e geram danos às vítimas. Muitos usuários de deepnudes não se sentem culpados a respeito disso por acreditarem que a imagem não é real e não machuca ninguém, portanto, não seria diferente do pornô tradicional. É necessário um processo educativo que reforce que o **consentimento** sobre as imagens geradas não é negociável.

Fonte: Home Security Heroes

Denúncia

É possível denunciar em **delegacias especializadas em crimes cibernéticos** ou **delegacias da mulher**. Também é possível denunciar na *Central Nacional de Denúncia de Crimes Cibernéticos* da ONG Safernet: https://new.safernet.org.br/denuncie.

Além disso, há um canal de acolhimento para as vítimas de violência online disponível em:
https://www.canaldeajuda.org.br/helpline

STALKING
PERSEGUIÇÃO ONLINE

O crime de stalking, que em português significa “perseguição”, é caracterizado pela perseguição constante, seja por meios tradicionais, seja por digitais, como a internet (ciberstalking ou perseguição online), que coloca em risco a integridade física e emocional da vítima, além de invadir sua privacidade e liberdade.

Muitos casos incluem o rastreamento da localização da vítima ou conhecidos da vítima por redes sociais, o monitoramento de suas atividades online e no mundo real.

Identificação

A pessoa que pratica a perseguição online pode ser alguém que você não conhece, alguém que você conheceu, um amigo, um familiar, um cuidador, ou até mesmo um parceiro ou ex-parceiro.

Nas redes sociais:

Stalking pode ser caracterizado por alguém que não aceita um “não” como resposta, mesmo depois de você deixar claro que não está interessada. Ou alguém que interage com todas as suas postagens e envia mensagens ou comentários constantes, ameaçadores ou exigentes. Ele também pode começar a contatar seus amigos ou familiares.

No celular:

Como o *stalkerware* (softwares espiões instalados pelo *stalker* ou *perseguidor* no aparelho da vítima) funciona em segundo plano, não há um método 100% seguro para detectá-lo.
No entanto, você deve ficar atenta aos seguintes sinais:

- A bateria do celular acaba mais rápido do que o normal.
- O dispositivo liga e desliga sozinho.
- Mudanças nas configurações do telefone sem explicação.
- Presença de aplicativos estranhos, especialmente aqueles com permissões para rastrear sua localização ou outras atividades.
- Aumento inesperado no consumo de dados.
- Alguém demonstrando um conhecimento incomum sobre sua vida, como onde você esteve ou detalhes de conversase mensagens privadas.

No computador:

Se você suspeitar que seu computador esteja infectado com *stalkerware*, é melhor usar uma ferramenta antivírus para escanear o computador e detectar o software.

Remoção

Não se esqueça! **Você deve primeiro buscar ajuda antes de remover o *stalkerware***, já que o simples ato de se livrar do software pode incentivar o agressor a intensificar a situação, representando um risco à sua segurança. Além disso, é **importante preservar provas do *stalkerware*** para possíveis ações legais. Assim algumas das ações imediatas recomendadas antes da remoção do software são:

- Substitua o aparelho comprometido ou use outro dispositivo, se possível.
- Procure aplicativos suspeitos ou configurações alteradas no seu celular.
- Em situações de abuso doméstico, procure a ajuda de ONGs que oferecem suporte às vítimas.

Para quem acredita que pode remover o *stalkerware* de forma segura, aqui estão algumas sugestões:

- Utilize um software antivírus para escanear o dispositivo e eliminar qualquer ameaça.
- Desinstale todos os aplicativos desconhecidos ou que você não tenha instalado.
- Verifique se o sistema operacional do dispositivo está atualizado.
- Realize uma restauração de fábrica para apagar o dispositivo completamente, incluindo qualquer *stalkerware.*

Prevenção

Selecione, se possível, a opção de conta privada em redes sociais. Não compartilhe seu nome completo, endereço ou número de telefone em posts e comentários e não divulgue sua rotina nas redes sociais.

Não aceite solicitações de amizades ou seguidas de pessoas que você não conhece nas redes sociais e evite responder ou ter qualquer tipo de contato com a pessoa que está te perseguindo ou assediando, pois isso pode encorajá-la a continuar tentando estabelecer algum tipo de comunicação com você.

Proteja todos os seus dispositivos com senhas fortes e individuais. Use senhas difíceis de adivinhar e armazene-as em um gerenciador de senhas protegido por senha. Altere, pelo menos a cada 3 meses, as senhas do seu e-mail, redes sociais, contas bancárias e qualquer outra conta importante e ative a autenticação multifatorial para suas contas.

Certifique-se de manter seus dispositivos sempre com você ou fisicamente protegidos.

Baixe apenas aplicativos de fontes oficiais e seguras, como a App Store da Apple.

Utilize um antivírus ou software de segurança em todos os seus dispositivos.

Ative os recursos de segurança nos seus dispositivos como o bloqueio de instalação de aplicativos de “fontes desconhecidas” no Android.

Sempre atualize todos os sistemas operacionais e aplicativos nos seus dispositivos.

Evite fazer root (para Android) ou jailbreak (para iPhones) já que podem comprometer a segurança do dispositivo.

Denúncia

Guarde todas as evidências que tiver (mensagens, e-mails, fotos, vídeos) e bloqueie o stalker nas suas redes sociais e faça uma denúncia diretamente na plataforma.

Stalking é crime!

O stalking é crime no Brasil e é previsto pela Lei 14.132, de 2021. A punição para quem pratica esse crime pode ser de seis meses a dois anos de prisão, além de multa.

Se você estiver sendo alvo de stalking, é importante denunciar o agressor à polícia. Você pode realizar a denúncia online, pelo site da Polícia Civil (PC), ou diretamente em **delegacias especializadas em crimes cibernéticos** ou **delegacias da mulher**.

DISCURSO DE ÓDIO E VIOLÊNCIA POLÍTICA DE GÊNERO ONLINE

O discurso de ódio é geralmente definido como manifestações que atacam e incitam ódio contra determinados grupos sociais baseados em raça, etnia, gênero, orientação sexual, religião ou origem nacional.

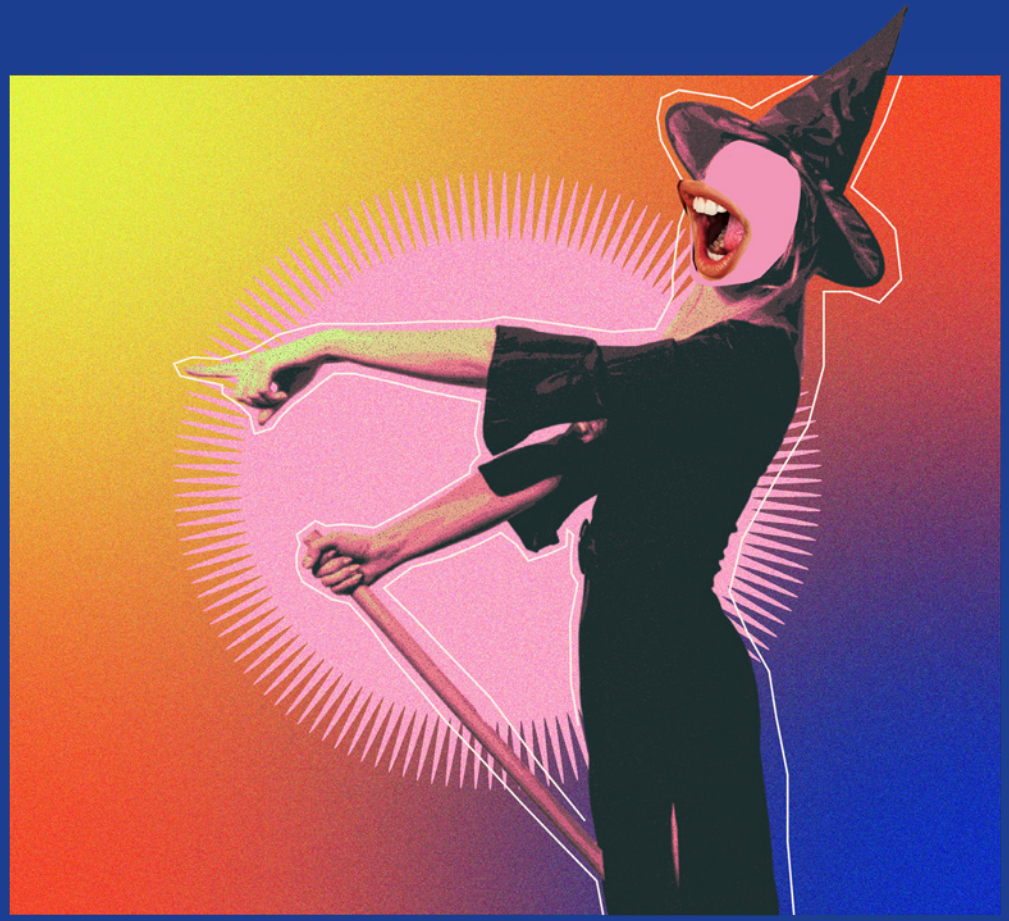
Quando o discurso de ódio baseado em gênero é propagado em períodos eleitorais contra candidatas e mulheres que atuam na política institucional, caracteriza-se a violência política de gênero.

Identificação

Em geral, o discurso de ódio tem conteúdo racista, misógino ou que incita a violência contra um determinado público. Os ataques políticos, por sua vez, se caracterizam pela tentativa de inferiorização de candidatas e uso de termos historicamente agressivos contra mulheres.

Uma dessas formas é a desinformação fundamentada em questões de gênero, uma vertente de violência política de gênero que busca minar a liberdade de expressão e enfraquecer a democracia. Mesmo aquelas que alcançam votações históricas na vida política são sujeitas a uma variedade de ataques pelo simples fato de serem mulheres.

Existe uma acentuação de estereótipos sexistas e fomento de atitudes misóginas, de modo a desencorajar as gerações mais jovens de buscar cargos públicos ou ingressar na esfera pública.



A Confederação Nacional de Municípios, em parceria com o Movimento de Mulheres Municipalistas, ouviu 224 prefeitas, em um universo de 677, e 210 vice-prefeitasde um total de 898, entre os meses de agosto e outubro de 2024.

+60%

sofreram algum tipo de violência política de gênero durante a campanha ou mandato.

49,1%

sofreram violência verbal

45,2%

sofreram violência psicológica

5,6%

sofreram violência física

O projeto De Olho nas Urnas revelou que houve um aumento na violência política contra mulheres entre 2020 e 2024.

Notícias de violência política durante o mês de convenções partidárias

13 em 2020

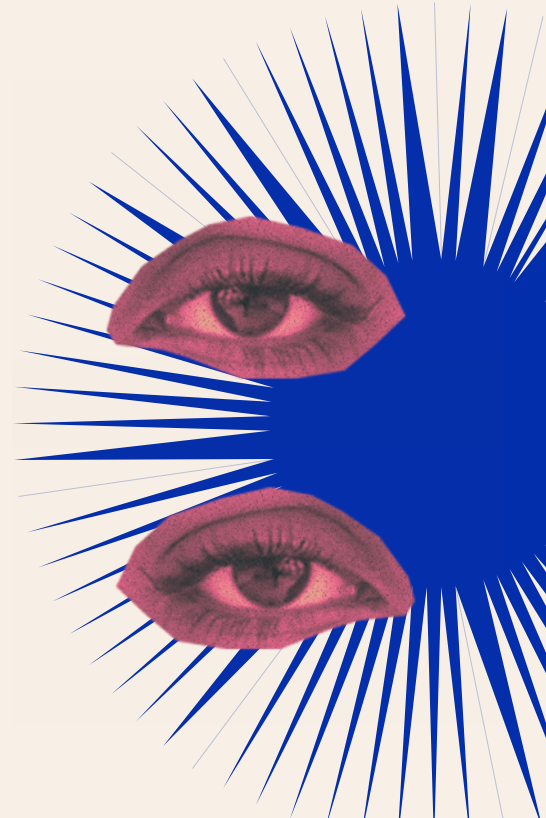
28 em 2024

Ocorrências noticiadas de violência política contra as candidatas o mês anterior às eleições municipais

29 em 2020

50 em 2024

O aumento pode estar relacionado ao maior número de denúncias, por parte da imprensa e no que se refere à aplicação da Lei 14.192/2021, que tornou crime a violência política de gênero.



Prevenção

Não alimente o ódio.

A interação com esse tipo de conteúdo é o que faz a mensagem viralizar e atingir mais pessoas, além de gerar receita para eventuais campanhas de apoio a esse tipo de discurso. Portanto, não dê palco ao discurso de ódio, nem mesmo para denunciar o conteúdo ou expressar sua indignação e discordância. O bom debate é aquele que evita ataques pessoais e usa argumentos e não apela para estereótipos e preconceitos contra grupos específicos.

Denúncia.

O discurso de ódio pode constituir crimes diversos, como injúria, calúnia, difamação, ameaça, entre outros, a depender da mensagem que for emitida. Nesses casos, a denúncia deve ser feita às autoridades competentes para investigação, em geral nas delegacias de polícia.

Já as condutas de violência política de gênero que se enquadrem na Lei 14.192/2021 são estritamente de cunho eleitoral, devendo ser denunciadas aos tribunais eleitorais competentes para investigação e punição dos envolvidos.

Prevenção

DOXXING

VAZAMENTO DE DADOS

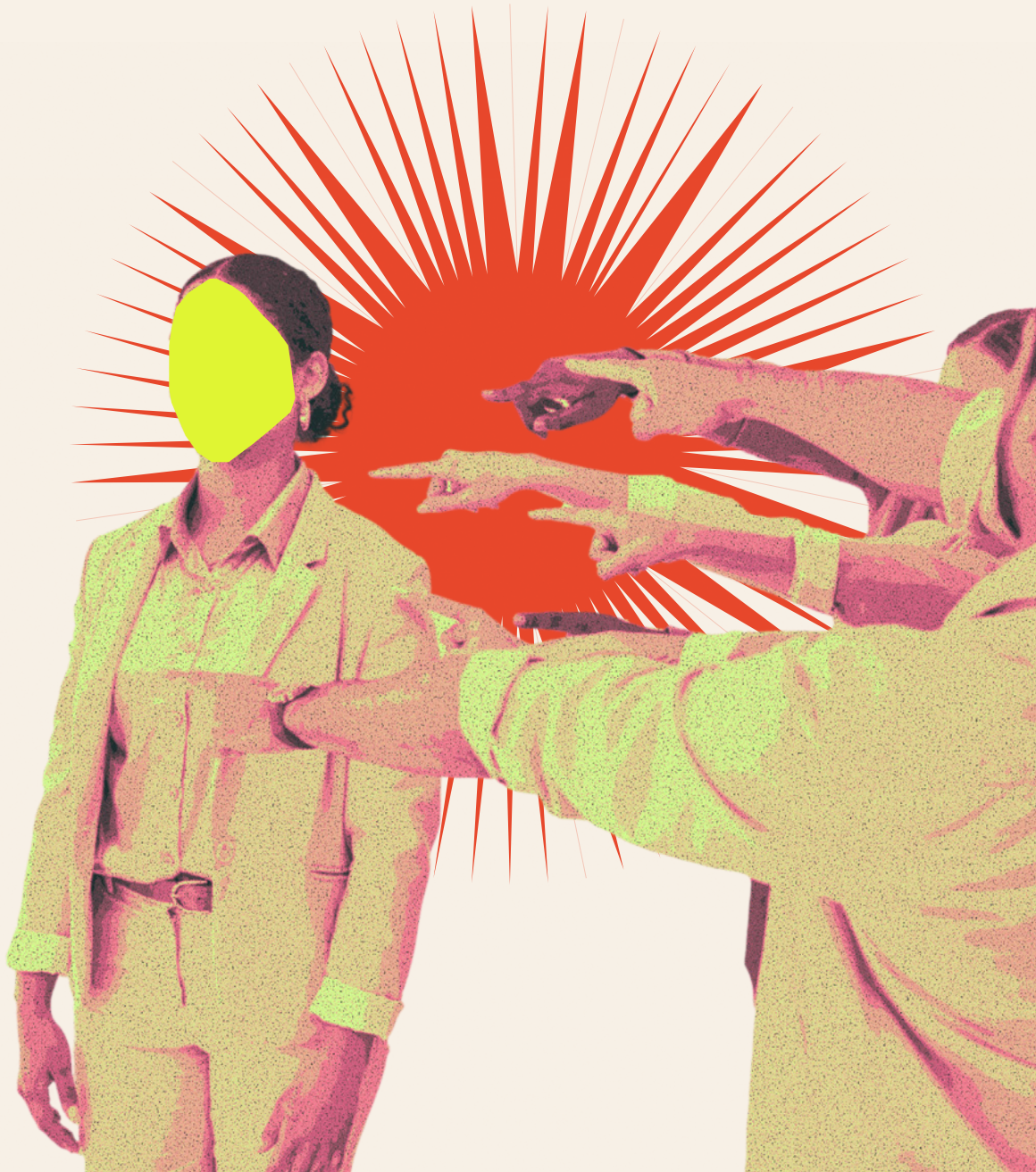
Doxing ou doxxing é a exposição não autorizada de dados pessoais de uma pessoa, ou até de seus familiares, na internet, como seu nome completo, endereço, local de trabalho, número de telefone, informações bancárias e outros detalhes privados. Essas informações são compartilhadas publicamente sem o consentimento da vítima.

Identificação

Uma das formas de se proteger é pesquisando sobre você ou determinada pessoa no Google e vendo o que se pode encontrar usando seu nome real ou de usuário em redes sociais e outros sites. Você ainda pode fazer uma busca inversa utilizando imagens e fotos pessoais.

Ah! Você também pode verificar se o seu e-mail esteve envolvido em grandes vazamentos de dados em https://haveibeenpwned.com/

Se for o caso, crie novas senhas fortes para o seu e-mail e para cada site identificado.



Prevenção

• Não abra e-mails de remetentes desconhecidos.

• Use VPN para que a sua localização não seja visível enquanto navega pela rede. Uma opção gratuita é o RiseUpVPN.

• Use senhas fortes, sempre lembrando de trocá-las a cada 3 meses. Use navegadores como o Firefox ou Brave que possuem funcionalidades que garantam uma maior privacidade.

• Use extensões que ajudam a bloquear rastreadores invisíveis de anunciantes e páginas na web como o Privacy Badger.

• Apague perfis em redes sociais e sites que você não usa mais.

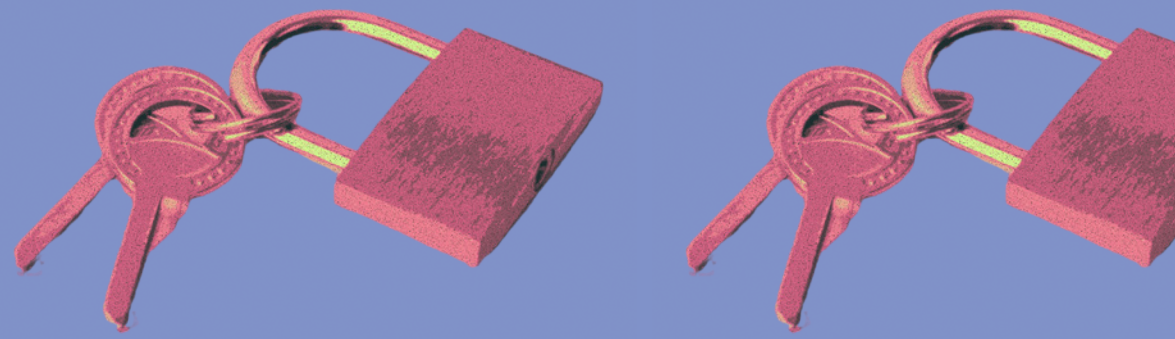
• Torne seu perfil privado nas redes sociais ativas e verifique quem te segue.

• Nada na internet é temporário. Uma postagem que você fez e depois excluiu pode ter sido salva em algum site que replica a rede social ou por alguém.

• Pense duas vezes antes de postar algo online ou de aceitar compartilhar suas informações com qualquer plataforma, especialmente dados sensíveis.

• Entenda que seus dados pessoais são qualquer informação que possa lhe identificar de forma direta ou indireta.

• Não compartilhe sua localização. Informações sobre lugares que você costuma visitar ou onde você mora são as mais sensíveis, já que podem ser facilmente exploradas por um stalker offline. Às vezes, a localização da nossa casa pode ser revelada até pelos aplicativos que usamos, como os de corrida, por exemplo.



Denúncia

O primeiro passo é fazer capturas de tela ou baixar as páginas onde suas informações foram divulgadas. Tente registrar a data e o URL de forma que fiquem visíveis.Faça o mesmo caso receba e-mails ou outras mensagens de assédio tentando manipulá-la ou extorqui-la. Esse registro é importante para sua própria referência e pode ser útil para as autoridades responsáveis pela investigação.

Também é essencial utilizar o canal de denúncias e denunciar nas plataformas da internet os posts ou publicações onde usuários não autorizados postaram suas informações pessoais. Embora as empresas se comprometam a remover esses posts, o doxxing não é uma prática definida pela legislação brasileira.

Entretanto, caso haja o vazamento de informações não públicas, o ato de doxxing pode configurar o crime de invasão de dispositivo informático, conforme o artigo 154-A do Código Penal. Se as informações forem públicas e acessíveis na internet, mas acompanhadas de ameaças, difamação ou injúrias, a conduta pode ensejar a aplicação dos artigos 147, 139 e 140 do Código Penal.

Instituto de Pesquisa em Direito & Tecnologia do Recife

NÃO É PARANOIA

Violência de gênero online não é paranoia. Meninas e mulheres precisam de espaços seguros nas ruas e na internet.

ip.rec.br

@ip.rec