

2019

White paper series  
Publicação 7

— COMBATE À VIOLÊNCIA ONLINE —  
**CONTRA A MULHER**  
UM CHAMADO POR PROTEÇÃO



**OEA** | Mais direitos  
para mais pessoas

**Canada** 



— COMBATE À VIOLÊNCIA ONLINE —

**CONTRA A MULHER**

UM CHAMADO POR PROTEÇÃO

# CRÉDITOS

**Luis Almagro**  
**Secretário-Geral**

da Organização dos Estados  
Americanos (OEA)

**Farah Diva Urrutia**

Secretaria de Seguridad Multidimensional

**Alejandra Mora Mora**

Secretária Executiva  
Comissão Interamericana de Mulheres (CIM)

**Alison August Treppel**

Secretária Executiva  
Comitê Interamericano contra o Terrorismo  
(CICTE)

**Betilde Muñoz-Pogossian**

Diretora do Departamento de Inclusão Social

## Equipe técnica

Belisario Contreras

Nathalia Foditsch

Kerry-Ann Barrett

Hilary Anderson

Pamela Molina

Claudia Gonzalez

Mariana Cardona

Miguel Angel Cañada

Rolando Ramirez

David Moreno

# CONTEÚDO

<b>1.</b>	<b>INTRODUÇÃO.....</b>	<b>5</b>
<b>2.</b>	<b>A VIOLÊNCIA ONLINE CONTRA A MULHER.....</b>	<b>7</b>
	A. QUAIS SÃO ALGUNS MÉTODOS UTILIZADOS NA VIOLÊNCIA ONLINE?	8
	QUADRO 1 DEEPFAKES – UMA NOVA ARMA CONTRA AS MULHERES	10
<b>3.</b>	<b>COMO ESSAS QUESTÕES ESTÃO SENDO TRATADAS NA AMÉRICA LATINA E NO CARIBE?.....</b>	<b>11</b>
<b>4.</b>	<b>MEDIDAS PRÁTICAS QUE PODEM SER TOMADAS IMEDIATAMENTE.....</b>	<b>13</b>
<b>5.</b>	<b>CONTEÚDO ÚTIL ONLINE.....</b>	<b>15</b>
<b>6.</b>	<b>REFERÊNCIAS.....</b>	<b>17</b>

— COMBATE À VIOLÊNCIA ONLINE —

**CONTRA A MULHER**

UM CHAMADO POR PROTEÇÃO

# Introdução

## 1

Enquanto cerca de metade da população mundial é composta de mulheres (**Banco Mundial, 2019**), apenas 48% delas têm acesso à internet (comparado com 58% dos homens) (**UIT, 2019**)<sup>1</sup>, e essa divisão digital é pior quando se adota uma perspectiva transversal, por exemplo de gênero e raça, etnia, deficiência e idade. Essa divisão tem importantes consequências no empoderamento e desenvolvimento da mulher, assim como nas sociedades, economias e no mundo dos negócios.

O conceito de alfabetização digital se refere tanto às habilidades técnicas necessárias, quanto à capacidade que se tem para interagir com conteúdo online de maneira crítica (**UNICEF, 2017**). Além disso, a **GSMA (2015)** identificou, por exemplo, que muitas mulheres em países em desenvolvimento não têm noção da profundidade e abrangência do que a internet poderia lhes oferecer em termos de conteúdo, já que elas estão presas em “ilhas de aplicativos”, o que significa que o que elas entendem como sendo “a internet” é o que elas veem através de um número limitado de aplicativos para dispositivos móveis. Ter habilidades adequadas de alfabetização

digital é essencial, especialmente considerando que o acesso e uso à internet criou muitas possibilidades que nunca poderíamos ter imaginado. De fato, a internet teve um impacto significativo em como nos comunicamos, como acessamos informação, como entendemos nossas próprias identidades.

Quando não há a real alfabetização digital, as mulheres não estão plenamente conscientes dos riscos envolvidos em usar a internet. De fato, mesmo com a gama de oportunidades que a internet traz, sua adoção e seu uso também vêm acompanhados de desafios, como a necessidade de melhores medidas de privacidade e segurança, já que nossas vidas são cada vez mais vividas através de nossas identidades online. Um exemplo de como as mulheres podem involuntariamente se expor na internet são os vazamentos de dados. Em 2019, mais de 12 milhões de históricos médicos hospedados por uma agência governamental relacionada à saúde reprodutiva da mulher foram expostos online na Índia. O assunto foi tratado pelo Computer Emergency Response Team (CERT) do país em conjunto com um pesquisador estrangeiro, mas demorou

<sup>1</sup> Apesar desses números serem estimativas, já que muitos países não submetem dados desagregados de gênero para a União Internacional de Telecomunicações - ITU (Web Foundation, 2018).

semanas até ser resolvido **(Cimpanu, 2019)**. A exposição de dados pessoais da mulher em si é uma violação de seu direito à privacidade, mas isso adicionalmente faz com que as mulheres estejam mais suscetíveis a diferentes tipos de violência e assédio online.

Ainda não temos um consenso na definição que se dá à multiplicidade de comportamentos que constituem a “violência online” contra a mulher, mas em geral ela é relacionada a comportamentos contra uma mulher específica. Ela pode ocorrer, por exemplo, quando uma mulher recebe uma mensagem direta através da internet ou tem suas informações disseminadas pela internet sem o seu consentimento, potencialmente causando uma gama negativa de sentimentos traumáticos **(PRC, 2018)**. Dada a importância atual do tópico e a demanda crescente por uma estrutura legal e regulatória que aborde de maneira mais efetiva a violência online contra a mulher, este Relatório tem o objetivo de destacar a necessidade de combater essa violência. O relatório explica brevemente como as mulheres podem ser assediadas online e resume alguns dos maiores problemas nas esferas pública e privada. Ele também brevemente avalia como essas questões têm sido tratadas na América Latina e no Caribe. Por último, ferramentas fornecem medidas práticas que podem ser seguidas por mulheres que desejam se proteger dos riscos de se expor online.



# A violência contra a mulher

## 2

A Convenção Interamericana para Prevenir, Punir e Erradicar a Violência Contra a Mulher de 1994 (Convenção de Belém do Pará) define a violência contra a mulher como sendo “qualquer ato ou conduta baseado no gênero, que cause morte ou sofrimento físico, sexual ou psicológico à mulher, tanto na esfera pública como na esfera privada” (artigo 1).<sup>2</sup> Quando a Convenção foi escrita e adotada no começo dos anos 90, a “esfera pública” não incluía o mundo online. A sociedade, contudo, mudou radicalmente nos últimos 25 anos e nossas identidades, atividades e interações online são um componente cada vez mais importante na nossa vida pública, especialmente para figuras políticas, jornalistas e outras pessoas que vivem a maior parte de suas vidas na esfera pública. Nossa atividade online também tem contribuído para que a linha entre as esferas pública e privada não fiquem tão claras, visto que, para alguns, a distinção talvez já não seja mais útil.

O sistema interamericano de direitos humanos ainda não estabeleceu uma definição para a multiplicidade de comportamentos que constituem a “violência online” contra a mulher dentro da estrutura de instrumentos legais já existentes, como a Convenção de Belém do Pará, e há uma necessidade urgente de se estabelecer esses

critérios para que possamos fornecer uma base sólida, conceitual e normativa para políticas públicas, e outras ações que têm como objetivo lidar com a violência online contra a mulher.

Em termos concretos, a violência online ocorre de diferentes maneiras. Ela “pode envolver e-mails ameaçadores ou de assédio, mensagens instantâneas ou posts de informações online” (**RPC, 2018**) e “dirige-se a uma pessoa específica ao entrar em contato diretamente com ela ou ao disseminar suas informações pessoais, causando “sofrimento, medo ou raiva” (**RPC, 2018**). Alguns termos equivalentes também usados são: “assédio online” e “assédio virtual”. Para efeitos deste artigo, incluímos qualquer tipo de assédio ou abuso sob o termo mais abrangente “violência online contra a mulher”.

O **Pew Research Center (2017)** define seis comportamentos diferentes que ele classifica como “assédio online”, que são: “xingamento”, “constrangimento intencional”, “ameaça física”, “assédio contínuo”, “assédio sexual” e “perseguição” (*stalking*). **Citron (2014)** descreve que o “assédio cibernético” “inclui ameaças de violência, invasão de privacidade, mentiras que ferem a reputação, pedido para que estranhos fisicamente machuquem a vítima

<sup>2</sup> <https://www.oas.org/en/mesecvi/convention.asp>

e ataques tecnológicos” (p. 3). As consequências de tais assédios causam sofrimento psicológico, dano à reputação e medo de efeitos no mundo real, e o problema é ainda mais prevalente entre mulheres (**Pew Research Center, 2017 e INEGI, 2015**).

Redes sociais podem ser usadas como uma ferramenta para o assédio. Um estudo conduzido pela **Amnistía Internacional (2019)** mostrou que é mais provável mulheres serem assediadas ou abusadas no Twitter, com “ameaças diretas ou indiretas de violência física ou sexual, abuso discriminatório contra um ou mais aspectos da identidade da mulher, assédio direcionado e violações de privacidade como o doxing, ou o compartilhamento de imagens sexuais ou íntimas de uma mulher sem o seu consentimento”. Enquanto os tribunais ainda estão tentando entender as diferenças, muitas vezes sutis, entre a livre expressão/discurso livre protegido e o que constitui uma “verdadeira ameaça” (**Drake, 2015**), muitas mulheres não se sentem seguras online, e sofrem violações de seus direitos humanos de viver livre de violência, seu direito à integridade física, mental e moral, e à privacidade.

O abuso discriminatório pode ser pior quando a mulher pertence à uma população indígena, é uma pessoa com deficiência ou qualquer outra identidade interseccional. Além do mais, considerando quanto dos nossos dados e informações estão online, o tempo que passamos online, e também o fato de que dependemos da internet para diferentes tipos de interações sociais e profissionais, o problema de assédio está se tornando mais comum do que nunca, aumentando a necessidade de uma resposta imediata que seja legalmente robusta e tecnicamente aplicável.

## a. Quais são alguns métodos utilizados na violência online?

- **“Cyberbullying”** ○ **Cyberbullying Research Center**, citando **Hinduja y Patchin (2014)**, lo define como sendo “o dano proposital e repetido infligido através do uso de computadores, celulares e outros dispositivos eletrônicos”, destacando sua natureza repetitiva. A **Ipsos (2018)** identificou que a conscientização da questão tem aumentado nos últimos anos. Entretanto, meninas adolescentes têm mais probabilidade de relatar serem vítimas de cyberbullying do que meninos (**Patchin, 2016**). Adicionalmente, **Betts et al. (2017)** identificaram um impacto negativo em como o valor de aprendizado é percebido entre mulheres que são sujeitas ao bullying, o que não acontece no mesmo grau entre homens. **Kwon et al. (2019)** descobriram que ser vítima de cyberbullying está correlacionado com a má qualidade de sono, o que pode levar a uma maior probabilidade de depressão entre adolescentes.

- **“Cyberstalking”** - A Privacy Rights Clearinghouse explica que um tipo de assédio online é o cyberstalking, que “envolve usar meios eletrônicos para perseguir a vítima, e geralmente se refere a um padrão de ameaças ou comportamentos maliciosos” (**PRC, 2018**). Há várias definições para o termo, e em alguns casos a ameaça precisa ser considerada real, e em outras, uma ameaça implícita já se encaixa na categoria (**RPC, 2018**). É relativamente fácil perseguir uma pessoa, já que muitas pessoas têm várias contas em redes sociais e uma significativa presença online. Ademais, muitas pessoas não conhecem bem os recursos de privacidade das plataformas que utilizam.

- **“Cyber Mobs”** é um conceito que ocorre quando grupos postam conteúdo ofensivo/destrutivo online, muitas vezes competindo com outros grupos, com a intenção de envergonhar alguém (**Citron, 2014**). Um exemplo de como isso afeta as mulheres foi apresentado pela é um conceito que ocorre quando grupos postam conteúdo ofensivo/destrutivo online, muitas vezes

competindo com outros grupos, com a intenção de envergonhar alguém (Citron, 2014). Um exemplo de como isso afeta as mulheres foi apresentado pela **Coding Rights e InternetLab (2017)** em que uma artista brasileira do estado da Bahia (nordeste do Brasil) estava na liderança em uma competição online quando uma cybermob foi organizada contra ela, votando em massa para seu competidor, deixando-a em 2º lugar na competição.

- **“Doxing/Doxxing”**: O termo “Dox” vem de “documentos”/ “.doc” e doxing é “recolher e publicar, muitas vezes através de hacking, as informações pessoais de uma pessoa, incluindo, entre outros, nomes completos, endereços, números de telefone, e-mails, nome de cônjuge e de filhos, detalhes financeiros” (**Women’s Media Center, 2019**). A Anistia Internacional relatou que em 2017 um quarto das mulheres tinham sido sujeitas à doxing pelo menos uma vez (**Amnistia Internacional, 2017**).

- **“Roubo de Identidade”** Ocorre quando os dados pessoais de uma pessoa são usados de maneira fraudulenta por outra pessoa (**Women’s Media Center, 2019**). Por exemplo, uma mulher russa descobriu que suas fotos estavam sendo usadas para outra conta no Twitter que havia viralizado, e demorou algum tempo até que ela conseguisse totalmente recuperar a sua identidade (**Kochetkova, 2016**). O roubo de identidade como esse pode ter consequências práticas e psicológicas que duram mais tempo do que se imagina.

- **“Pornografia de vingança” / “Pornografia não-consensual”** – É “a divulgação de imagens com conteúdo sexual de indivíduos sem o seu consentimento” e isso inclui imagens/vídeos que foram adquiridos com ou sem consentimento (**Netizens, 2019**). Esse cenário é particularmente prejudicial para mulheres, já que seus corpos e sexualidade estão sujeitos a normas culturais que são, em muitos casos, misóginas. Um conceito relacionado é o de “sextorsão”,

no qual dinheiro ou outras exigências são feitas para não divulgar fotos ou vídeos com conteúdo sexual explícito. Considerando que em alguns países mais de 80% dos adultos já enviaram mensagens de texto com algum tipo de conteúdo sexual explícito (**Stasko y Geller, 2015**), muitas pessoas correm o risco de sofrer esse tipo de violência online.

## QUADRO #1 Deepfakes Uma nova arma contra as mulheres

“Deepfakes” são vídeos que usam técnicas de aprendizado de máquina para trocar o rosto de uma pessoa para outra (Knight, 2019). Tais tecnologias surgiram em 2017 (Deeprtrace, 2019) e estão sendo utilizadas em diferentes contextos, mas os mais comuns estão relacionados à política e pornografia. O número de vídeos deepfake online está crescendo exponencialmente e isso se deve parcialmente ao fato de que agora é mais fácil para não-especialistas usar certas tecnologias (Deeprtrace, 2019). O Departamento de Defesa dos Estados Unidos está até desenvolvendo ferramentas para automatizar ferramentas de perícia com o objetivo de identificar deepfakes (Knight, 2019).

De acordo com Deeprtrace (2019), as mulheres são os principais alvos quando deepfakes são usados em pornografia. Casos envolvendo o uso dessa tecnologia para atacar mulheres na política também estão começando a aparecer. Um exemplo é uma famosa política, que em 2019 apareceu em um vídeo como se estivesse bêbada. O vídeo rapidamente viralizou no Facebook (Rosenberg, 2019). Isso é particularmente preocupante dado o fato de que se espera que os deepfakes tenham um impacto sério nas eleições futuras em todo o mundo (Parkin, 2019).

Enquanto todas as mulheres correm o risco de sofrer assédio online, outros aspectos de identidade (raça, etnia, idioma, orientação sexual ou identidade de gênero, condição de imigrante e deficiência, entre outros) podem agravar o problema. Mulheres que pertencem a diversas identidades simultaneamente estão mais vulneráveis para a violência online. Como explica o Women’s Media Center (2019), uma mulher homossexual pode sofrer homofobia, enquanto uma mulher negra pode sofrer racismo, em ambos os casos adicionalmente sofrendo o sexismo. Isso destaca a importância de olhar para a violência online contra a mulher de uma perspectiva interseccional.

Mulheres que têm uma vida política também são muitas vezes alvos de assediadores online. A Organização dos Estados Americanos (OEA) adotou a Declaration on Political Harassment and Violence against Women (Declaração sobre Assédio Político e Violência Contra a

Mulher) em 2015, que reconhece os “fatores estruturais que afetam a violência contra a mulher e padrões socioculturais e simbólicos, assim como estereótipos sociais e culturais que os perpetuam” (OAS, 2015). A declaração incentiva redes sociais, entre outras partes interessadas, a adotar medidas que possam eliminar a discriminação e estereótipos sexistas (OAS, 2015). Isso é particularmente importante já que debates políticos acontecem cada vez mais nas plataformas de redes sociais, e atualmente muitas pessoas recebem a maior parte de suas notícias políticas através dessas plataformas.

Através dessa visão geral, é possível concluir que as mulheres são atingidas através de vários métodos e tecnologias. Uma breve descrição de como algumas dessas questões estão sendo tratadas na América Latina e em países do Caribe está apresentada abaixo.

# Como essas questões estão sendo tratadas na América Latina e no Caribe?



Houve avanços nos últimos anos por toda a América Latina e países do Caribe para combater a violência online contra a mulher. Quanto à legislação contra a “pornografia de vingança”, por exemplo, a lei de número 13.772/2018<sup>3</sup> foi promulgada em dezembro de 2018 no Brasil, mudando a legislação anterior para criminalizar a gravação não-autorizada e divulgação de imagens de pessoas nuas ou com conteúdo sexual. Segundo a lei, tais atos agora são considerados “violência doméstica” em casos em que havia um relacionamento prévio entre a vítima e seu agressor. A mídia teve um papel crucial em promover o debate contra a pornografia de vingança depois de casos concretos terem ocorrido. Tais debates levaram a mudanças na legislação que diretamente tratasse a questão **(Neris et. al, 2018)**. Argentina, Chile, México e Uruguai são exemplos de estados-membros da OEA que atualmente discutem redigir projetos de lei que lidam com a pornografia de vingança **(Neris et. al, 2018)**. O México, em particular, propôs uma emenda ao seu Código Penal e Lei Geral do Acesso à Mulher a uma Vida Livre de Violência<sup>4</sup> que trata do assédio cibernético contra a mulher **(Cruz, 2019)**.

Além do mais, vários países por toda a América Latina aprovaram legislação sobre assédio político contra a mulher (Bolívia) ou estão discutindo redigir projetos de lei (Costa Rica, Equador, Honduras, México e Peru) **(OEA, 2017)**. SDe acordo com o que foi descrito acima, isso é importante, entre outras razões, pelo impacto da tecnologia em debates democráticos.

Quanto à questão de polícia especializada em crimes cibernéticos e/ou a violência online contra a mulher, avanços também foram vistos nos últimos anos. O México tem uma divisão de sua polícia que é especificamente focada em crimes cibernéticos, lidando com crimes de violência online<sup>5</sup>, e um portal governamental tem conteúdo específico com a intenção de conscientizar sobre o cyberbullying<sup>6</sup>. No Brasil, alguns estados têm delegacias de polícia especializadas, outros não.<sup>7</sup> No Peru, qualquer um pode denunciar a violência online através de um formulário online, mesmo que a pessoa que esteja denunciando não seja a vítima.<sup>8</sup>

<sup>3</sup> <https://www2.camara.leg.br/legin/fed/lei/2018/lei-13772-19-dezembro-2018-787488-publicacaooriginal-157031-pl.html>

<sup>4</sup> Ley General de Acceso de las Mujeres a una Vida Libre de Violencia

<sup>5</sup> <http://www.ssp.df.gob.mx/ciberdelincuencia.html>

<sup>6</sup> <https://www.gob.mx/ciberbullying>

<sup>7</sup> <https://new.safernet.org.br/content/delegacias-cibercrimes>

<sup>8</sup> <http://www.noalacosovirtual.pe/>

Isso não é tudo que está acontecendo na América Latina e nos países do Caribe. Na verdade, é um breve resumo com a intenção de demonstrar a complexidade da questão. É possível notar que países estão se movendo na direção de reconhecer e definir o problema, assim como aumentar a proteção para mulheres online. Ao mesmo tempo, há novos métodos e novas tecnologias surgindo, e vários tipos de violência online estão sendo colocados em prática todos os dias.

Com o objetivo de contribuir para melhor proteger as mulheres online, este Relatório termina com uma série de medidas práticas que podem ser tomadas pelas mulheres, assim como recursos úteis que estão disponíveis online.

# Medidas práticas que podem ser tomadas imediatamente

## 4

Começar com as medidas descritas abaixo é uma boa ideia se você gostaria de se proteger contra a violência online. Conteúdo online úteis também podem ser encontrados abaixo. Entre esses conteúdos, há guias e manuais que podem ajudar a entender melhor o que é a violência online contra a mulher, e quais medidas podem ser tomadas contra ela.

### | Medidas Preventivas: |

- **Use senhas fortes e não as compartilhe com ninguém.** Assegure-se de ter senhas fortes e não as compartilhe com ninguém. Adicionalmente, não use a mesma senha em diferentes plataformas e serviços. Para mais informações, acesse **OEA (2019)** “Password Do’s and Don’ts” (p. 11).

- **Aprenda a entender e mudar as configurações de privacidade nas plataformas de redes sociais.** Parte das informações expostas online podem ser controladas nas configurações de segurança. É importante saber quais são as opções em termos de proteger a sua privacidade. Por exemplo, é importante manter seus posts privados para que pessoas que não façam parte dos seus contatos não tenham acesso ao conteúdo que você posta, e usar a autenticação de dois fatores para fazer o login. Para mais informações, acesse a **OEA (2019)** “Check Your Privacy Settings” (p. 09).

- **Use aplicativos de mensagens criptografadas para se comunicar.**

Aplicativos criptografados são uma opção mais segura, já que fica mais difícil alguém acessar o conteúdo que é modificado através dele. Enquanto mensagens de texto normais não são criptografadas, aplicativos como *Signal*, *Telegram*, *WhatsApp* y *Wire* sí lo están.

- **Use uma Rede Privada Virtual (VPN) para criptografar seu tráfego online.**

Esse passo é especialmente importante quando você não está utilizando uma rede privada (quando está acessando a internet de um café ou outra rede de wi-fi pública, por exemplo). Serviços de VPN permitem que o seu tráfego seja criptografado para que outras pessoas que estejam usando a rede não vejam o que você está fazendo online. Mesmo que a maioria de serviços de VPN não sejam de graça, eles são um bom investimento. Para mais informações acesse a **OEA (2019)** “VPN Use” (p. 13).



## **Se violência/assédio/ameaça/abuso ocorrer:**

• **Guarde as provas de violência/assédio/ameaça/abuso.** Não apague essas provas. É essencial manter qualquer mensagem que tiver ou outra forma de prova, como captura de telas, que podem ser usadas para provar a/o violência/assédio/ameaça/abuso.

• **Denuncie a violência à plataforma/serviço online.** ENa maioria dos casos, é possível denunciar a violência à plataforma/serviço online em si. Denuncie o que ocorreu imediatamente. A plataforma investigará para determinar se o conteúdo trocado viola os “padrões da comunidade” existentes, e pode ou não tomar medidas para remover o conteúdo e/ou restringir os privilégios e atividade de quem cometeu o ato. Cada plataforma tem suas próprias regras, mas você pode ver um exemplo de como retirar conteúdo e outros aspectos de aplicação das regras ao acessar a **OEA (2019)** “Enforcement of Our Rules” (p. 28).

• **Não responda qualquer mensagem que contenha ameaça/assédio.** É importante não “alimentar” a pessoa que está cometendo a violência. Não responda nenhuma mensagem que seja intimidadora/ameaçadora. Se possível, bloqueie a pessoa para que as mensagens não possam mais ser recebidas. Na maioria dos casos, a pessoa que você bloqueou não será notificada que você a bloqueou.

• **Entre em contato com as autoridades locais (Essa medida deve ser tomada com precaução, já que apenas ameaças graves devem ser denunciadas).** Além das autoridades policiais comuns, há autoridades policiais especializadas em muitos países, como a polícia especializada em crimes cibernéticos. Entre em contato com eles ou com

qualquer autoridade local que possa ajudar. Em alguns casos, há também divisões de polícia especializadas na violência contra a mulher, assim como formulários online que podem ser usados para fazer denúncias de violência online.

• **Procure ajuda de pessoas em quem confia e profissionais de saúde mental.** Ser vítima da violência online é perturbador e pode profundamente afetar a saúde mental e o bem-estar de uma pessoa. É importante ter apoio externo de profissionais e pessoas em quem confia. Eles podem ajudá-la a tomar as medidas adequadas para lidar com a situação.

• **Busque recursos online úteis.** Há manuais, ferramentas e uma grande variedade de material online que podem ser consultados. Algumas dessas ferramentas estão listadas abaixo na Seção 5. **“Conteúdo Útil Online”**. “Media Literacy and Digital Security” (**OAS, 2019**).



# Conteúdo Útil Online

## 5

### [Relatórios, Manuais e Ferramentas]

- Alfabetização e Segurança Digital. Melhores Práticas no uso do Twitter. OEA 2019 <https://www.oas.org/pt/ssm/cicte/docs/20190916-POR-Alfabetismo-y-seguridad-digital-Twitter.pdf>
- Acoso Online. Pornografía no consentida. Cinco claves para denunciar y resistir su publicación. 2017. (Espanhol) Fundación Datos Protegidos; Equipo Latinoamericano de Justicia y Género (ELA); InternetLab; Hiperderecho; Acceso Libre; Ipandetec; Son Tus Datos; Fundación Datos Protegidos Bolivia; No! to Online Abuse and Harassment (NOAH); Fundación Karisma; TEDIC. <https://acoso.online/cl/>
- A First Look at Digital Security. Access Now. 2018. (Inglês) <https://www.accessnow.org/your-spring-welcoming-gift-is-here-the-freshest-version-of-a-first-look-at-digital-security/>
- A toolkit for researching women’s internet access and use. A4AI; World Wide Web Foundation, GSMA and APC. 2018. (Inglês) <https://webfoundation.org/research/a-toolkit-for-researching-womens-internet-access-and-use/>
- Advancing Women’s Rights Online: Gaps and Opportunities in Research and Advocacy. World Wide Web Foundation. 2018. (Inglês) <https://webfoundation.org/research/advancing-womens-rights-online-gaps-and-opportunities-in-research-and-advocacy/>
- Online Harassment Field Manual. (PEN America. 2019. (Inglês) <https://onlineharassmentfieldmanual.pen.org/>
- Manuals with a Gender Perspective. Tactical Tech. (Inglês e Espanhol) [https://gendersec.tacticaltech.org/wiki/index.php/Manuals\\_with\\_a\\_gender\\_perspective](https://gendersec.tacticaltech.org/wiki/index.php/Manuals_with_a_gender_perspective)

- Violencia Cibernetica. Lersy G. Boria Vizacarrondo. Procuradora de las Mujeres, Puerto Rico. (Espanhol) <http://www.mujer.pr.gov/Educaci%C3%B3nPrevenci%C3%B3n/Opusculos/Violencia%20Cibernetica.pdf>
- Netizens Online Security Guide. 2019. (Inglês) <https://drive.google.com/file/d/0B-xwQoatiZyBVTZid3ZrdUk2R28/view>
- Safernet. Diferentes conteúdos relacionados ao assédio cibernético. (Português) <https://new.safernet.org.br/>

## | TEDTalks |

- How Online Abuse of Women Has Spiraled Out of Control. Ashley Judd. TEDTalk. 2016 (Inglês). [https://www.ted.com/talks/ashley\\_judd\\_how\\_online\\_abuse\\_of\\_women\\_has\\_spiraled\\_out\\_of\\_control/transcript?language=en](https://www.ted.com/talks/ashley_judd_how_online_abuse_of_women_has_spiraled_out_of_control/transcript?language=en)
- Anita Sarkeesian no TEDxWomen 2012. Anita Sarkeesian. 2012. (Inglês) <https://www.youtube.com/watch?v=GZAxwsg9J9Q>
- Grooming, el acoso ¿virtual? Sebastián Bortnik. TEDxRíodelaPlata. 2016. (Espanhol) <https://www.youtube.com/watch?v=0wZjKOulodo>

## | Documentários |

- Netizens. Cynthia Lowen. 2019. (Inglês) <https://www.netizensfilm.com/>

# Referências



Anistia Internacional. (2017). Amnistía revela alarmante impacto de los abusos contra las mujeres en Internet. Extraído de <https://www.amnesty.org/es/latest/news/2017/11/amnesty-reveals-alarming-impact-of-online-abuse-against-women/>

Anistia Internacional. (2019). Why Twitter is a toxic place for women. Extraído de <https://www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1/>

Betts, L. R., Spenser, K. A., & Gardner, S. E. (2017). Adolescents' Involvement in Cyber Bullying and Perceptions of School: The Importance of Perceived Peer Acceptance for Female Adolescents. *Sex Roles*, 77(7), 471–481. <https://doi.org/10.1007/s11199-017-0742-2>

Cimpanu, C. (n.d.). Indian govt agency left details of millions of pregnant women exposed online. ZDNet. Extraído de <https://www.zdnet.com/article/indian-govt-agency-left-details-of-millions-of-pregnant-women-exposed-online/>

Citron, D. K. (2014). *Hate Crimes in Cyberspace*. Harvard University Press.

Coding Rights, & InternetLab. (2017). Violências de gênero na Internet: Diagnóstico, soluções e desafios. Contribuição Conjunta Do Brasil Para A Relatora Especial Da ONU Sobre Violência Contra a Mulher. Extraído de [https://www.academia.edu/35642655/Viol%C3%AAncias\\_de\\_g%C3%AAnero\\_na\\_Internet\\_diagn%C3%B3stico\\_solu%C3%A7%C3%B5es\\_e\\_desafios](https://www.academia.edu/35642655/Viol%C3%AAncias_de_g%C3%AAnero_na_Internet_diagn%C3%B3stico_solu%C3%A7%C3%B5es_e_desafios)

Comparitech. (2019). Cyberbullying Statistics and Facts for 2016–2019. Extraído em 3 de novembro de 2019, do site da Comparitech: <https://www.comparitech.com/internet-providers/cyberbullying-statistics/>

Cruz, H. (2019). Proponen ley contra ciberacoso a la mujer. Extraído em 12 de novembro de 2019, from El Universal website: <https://www.eluniversal.com.mx/metropoli/proponen-ley-contra-ciberacoso-la-mujer>

Cyberbullying Research Center. (2014, December 23). What is Cyberbullying? Extraído em 3 de novembro de 2019, do site Cyberbullying Research Center: <https://cyberbullying.org/what-is-cyberbullying>

Deeptrace. (2019). The State of Deepfakes: Landscape, Threats and Impact. Extraído de <https://storage.googleapis.com/deeptrace-public/Deeptrace-the-State-of-Deepfakes-2019.pdf>

Drake, B. (n.d.). The darkest side of online harassment: Menacing behavior. Extraído em 3 de novembro de 2019, do site Pew Research Center: <https://www.pewresearch.org/fact-tank/2015/06/01/the-darkest-side-of-online-harassment-menacing-behavior/>

EQUALS. (n.d.). 10 Lessons Learnt: Closing the Gender Gap in Internet Access and Use Insights from the EQUALS Access Coalition. Extraído de [https://2b37021f0f4a-4640-8352-0a3c1b7c2aab.filesusr.com/ugd/04bfff\\_33ded6f6855b4de5b7a09186e1c6add7.pdf](https://2b37021f0f4a-4640-8352-0a3c1b7c2aab.filesusr.com/ugd/04bfff_33ded6f6855b4de5b7a09186e1c6add7.pdf)

Franceschi-Bicchierai, L. (2017, September 21). This Ransomware Demands Nudes Instead of Bitcoin. Extraído em 5 de novembro de 2019, do site Vice: [https://www.vice.com/en\\_us/article/yw3w47/this-ransomware-demands-nudes-instead-of-bitcoin](https://www.vice.com/en_us/article/yw3w47/this-ransomware-demands-nudes-instead-of-bitcoin)

GSMA. (2015). Accelerating Digital Literacy: Empowering women to use the mobile internet.

Hinduja, S., & Patchin, J. W. (2014). Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying (Second edition). Thousand Oaks, California: Corwin.

INEGI. (2015). Módulo sobre Ciberacoso 2015 MOCIBA Documento metodológico. 20.

InternetLab. (2018). Como países enfrentam a disseminação não consentida de imagens íntimas? Extraído em 4 de novembro de 2019, do site da InternetLab: <http://www.internetlab.org.br/pt/desigualdades-e-identidades/mapa-pornografia-de-vinganca/>

Ipsos. (2018). Global Awareness of Cyberbullying Is Increasing, Though 1 in 4 Adults Haven't Heard of It. Extraído de <https://www.ipsos.com/en-us/news-polls/global-awareness-of-cyberbullying>

ITU. (2019). ITU report on global digital connectivity finds gender digital gap is growing. Extraído de <http://digitalinclusionnewslog.itu.int/2019/11/05/itu-report-on-global-digital-connectivity-finds-gender-digital-gap-is-growing/>

Judd, A. (2015). Forget Your Team: Your Online Violence Toward Girls and Women Is What Can Kiss My Ass. Mic. Extraído de <https://www.mic.com/articles/113226/forget-your-team-your-online-violence-toward-girls-and-women-is-what-can-kiss-my-ass>

Knight, W. (2018). The Defense Department has produced the first tools for catching deepfakes. MIT Technology Review. Extraído de <https://www.technologyreview.com/s/611726/the-defense-department-has-produced-the-first-tools-for-catching-deepfakes/>

Kochetkova, K. (n.d.). Um caso assustador de roubo de identidade no Twitter. Retrieved October 12, 2019, from <https://www.kaspersky.com.br/blog/stolen-social-identity/5949/>

Kwon, M., Seo, Y. S., Dickerson, S. S., Park, E., & Livingston, J. A. (2019). 0802 Cyber Victimization and Depressive Symptoms: A Mediation Model Involving Sleep Quality. *Sleep*, 42(Supplement\_1), A322–A322. <https://doi.org/10.1093/sleep/zsz067.800>

Neris, N., Ruiz, J., & Valente, M. (2018). Enfrentando Disseminação Não Consentida de Imagens Íntimas: Uma análise comparada. Extraído de InternetLab website: [http://www.internetlab.org.br/wp-content/uploads/2018/05/Neris\\_Ruiz\\_e\\_Valente\\_Enfrentando1.pdf](http://www.internetlab.org.br/wp-content/uploads/2018/05/Neris_Ruiz_e_Valente_Enfrentando1.pdf)

Netizens. (2019). Netizens Online Security Guide. Extraído de [https://drive.google.com/file/d/0B-xwQoatiZyBVTZid3ZrdUk2R28/view?usp=embed\\_facebook](https://drive.google.com/file/d/0B-xwQoatiZyBVTZid3ZrdUk2R28/view?usp=embed_facebook)

OAS. (2015). Declaration on Political Harassment and Violence Against Women. Extraído de <http://www.oas.org/en/cim/docs/DeclaracionViolenciaPolitica-EN.pdf>

OAS. (2017). Fact Sheet—Violencia y acoso político contra las mujeres en el marco de la Convención de Belém do Pará. Extraído de <https://www.oas.org/en/cim/docs/ViolenciaPolitica-FactSheet-ES.pdf>

OAS. (2019). Media Literacy and Digital Security: Twitter Best Practices. Extraído de <https://www.oas.org/en/sms/cicte/docs/20190913-DIGITAL-ENG-Alfabetismo-y-seguridad-digital-Twitter.pdf>

Parkin, S. (2019). The rise of the deepfake and the threat to democracy. *The Guardian*. Extraído de <https://www.theguardian.com/technology/ng-interactive/2019/jun/22/the-rise-of-the-deepfake-and-the-threat-to-democracy>

Patchin, J. W. (2016). 2016 Cyberbullying Data. Extraído em 3 de novembro de 2019, do site do Cyberbullying Research Center: <https://cyberbullying.org/2016-cyberbullying-data>

Pew Research Center. (2017). Online Harassment 2017. Extraído em 12 de novembro de 2019, no site [https://www.pewinternet.org/wp-content/uploads/sites/9/2017/07/PI\\_2017.07.11\\_Online-Harassment\\_FINAL.pdf](https://www.pewinternet.org/wp-content/uploads/sites/9/2017/07/PI_2017.07.11_Online-Harassment_FINAL.pdf)

PRC. (2018). Online Harassment & Cyberstalking. Extraído em 5 de novembro de 2019, do site da Privacy Rights Clearinghouse: <https://privacyrights.org/consumer-guides/online-harassment-cyberstalking>

Rosenberg, A. (2019). Facebook exec's outrageous defense of the "drunk Pelosi" video doesn't add up. Extraído de <https://mashable.com/article/facebook-monika-bickert-drunk-pelosi-video/?europe=true>

Stasko, E. C., & Geller, P. A. (2015). Reframing Sexting as a Positive Relationship Behavior: (528002015-001) [Data set]. <https://doi.org/10.1037/e528002015-001>

Unicef. (2017). Access to the Internet and Digital Literacy. Extraído em 12 de novembro de 2019, do site [https://www.unicef.org/csr/css/UNICEF\\_CRB\\_Digital\\_World\\_Series\\_ACCESS.pdf](https://www.unicef.org/csr/css/UNICEF_CRB_Digital_World_Series_ACCESS.pdf)

Web Foundation. (2018a). Advancing Women's Rights Online: Gaps and Opportunities in Research and Advocacy. Extraído de [http://webfoundation.org/docs/2018/08/Advancing-Womens-Rights-Online\\_Gaps-and-Opportunities-in-Policy-and-Research.pdf](http://webfoundation.org/docs/2018/08/Advancing-Womens-Rights-Online_Gaps-and-Opportunities-in-Policy-and-Research.pdf)

Web Foundation. (2018b). Measuring the digital divide: Why we should be using a women-centered analysis. Extraído de <https://webfoundation.org/2018/05/measuring-the-digital-divide-why-we-should-be-using-a-women-centered-analysis/>

Women's Media Center. (2019). Online Abuse 101 — Women's Media Center. Extraído em 3 de novembro de 2019 do site <http://www.womensmediacenter.com/speech-project/online-abuse-101>

World Bank. (2019). Population, female (% of total population) | Data. Extraído em 12 de outubro de 2019 do site <https://data.worldbank.org/indicator/SP.POP.TOTL.FE.ZS>





OEA

Mais direitos  
para mais pessoas

Canada 

— COMBATE À VIOLÊNCIA ONLINE —  
**CONTRA A MULHER**  
UM CHAMADO POR PROTEÇÃO

White paper series  
**Publicação 7**

**2019**