2019

White paper series
Edición 7

COMBATIR LA VIOLENCIA EN LÍNEA CONTRA LAS MUJERES

UN LLAMADO A LA PROTECCIÓN

OEA Más derechos para más gente

Canada

— COMBATIR LA VIOLENCIA EN LÍNEA —

CONTRA LAS MUJERES

UN LLAMADO A LA PROTECCIÓN

CRÉDITOS

Luis Almagro
Secretario General
Organización de los Estados Americanos (OEA)

Farah Diva Urrutia
Secretaria de Seguridad Multidimensional

Alejandra Mora Mora
Secretaria Ejecutiva
Comisión Interamericana de Mujeres (CIM)

Alison August Treppel
Secretaria Ejecutiva
Comité Interamericano contra el Terrorismo (CICTE)

Betilde Muñoz-Pogossian
Directora del Departamento de Inclusión Social

Technical Team

Belisario Contreras
Nathalia Foditsch
Kerry-Ann Barrett
Hilary Anderson
Pamela Molina
Claudia Gonzalez
Mariana Cardona
Miguel Angel Cañada
Rolando Ramirez
David Moreno

CONTENIDO

— COMBATIR LA VIOLENCIA EN LÍNEA —

CONTRA LAS MUJERES

UN LLAMADO A LA PROTECCIÓN

Introducción

1

Aproximadamente la mitad de la población mundial está compuesta por mujeres **(Banco Mundial, 2019)**, pero solo el 48% de ellas tiene acceso a Internet (en comparación con el 58% de los hombres) **(UIT, 2019)**[1], y esta brecha digital se agrava aún más cuando se adopta una perspectiva transversal, p. ej. género y raza, etnia, discapacidad y edad. Esta grieta tiene implicaciones importantes en términos del empoderamiento y desarrollo de las mujeres, así como para las sociedades, las empresas y las economías. Además de las brechas en el acceso, la falta de habilidades en alfabetización digital sigue siendo una realidad para muchas mujeres.

El concepto de alfabetización digital se refiere tanto a las habilidades técnicas que se necesitan, como a la capacidad de interactuar con los contenidos en línea de manera crítica **(UNICEF, 2017)**. Además, la **GSMA (2015)** ha encontrado, por ejemplo, que muchas mujeres en países en desarrollo no comprenden la profundidad y amplitud de lo que podría ofrecerles el Internet en términos de contenido, ya que están atrapadas en unas "islas de aplicativos", o sea que, lo que entienden como el "Internet" es lo que ven a través de un cierto número de aplicativos móviles. Contar con habilidades adecuadas de alfabetización digital es clave, en especial si se tiene en cuenta que el acceso y el uso de Internet han creado incontables posibilidades que nunca hubiéramos imaginado. Ha afectado profundamente cómo nos comunicamos, cómo accedemos a la información y cómo entendemos nuestras propias identidades.

Al no tener una alfabetización adecuada, las mujeres no son plenamente conscientes de los riesgos que corren con el uso de Internet. De hecho, a pesar de la extensa gama de oportunidades que brinda, la adopción y el uso de Internet también se han visto acompañados por desafíos como la necesidad de fortalecer la privacidad y la seguridad, ya que nuestras vidas se desarrollan cada vez más a través de nuestras identidades en línea. Un ejemplo de cómo las mujeres pueden exponerse en línea involuntariamente es con las filtraciones de datos. En la India en 2019, más de 12 millones de registros médicos relacionados con la salud reproductiva de las mujeres, alojados por una agencia gubernamental, fueron expuestos en línea. El problema fue abordado por el

[1] Estas son cifras estimadas, ya que la mayoría de los países no le presentan a la Unión Internacional de Telecomunicaciones (UIT) datos desglosados por género (Web Foundation, 2018).

Equipo nacional de respuesta a emergencias informáticas (CERT) en cooperación con un investigador extranjero, pero tardó semanas en resolverse **(Cimpanu, 2019)**. La exposición de la información personal de las mujeres es en sí misma una violación de su derecho a la privacidad, pero también las hace más susceptibles a sufrir diferentes tipos de acoso y violencia en línea.

Todavía no nos hemos puesto de acuerdo con una definición de la multiplicidad de comportamientos que constituyen la "violencia en línea" contra las mujeres, aunque comúnmente se dice que son los comportamientos en contra de una mujer en particular. Puede ser, por ejemplo, cuando una mujer recibe un mensaje directo a través de Internet o se difunde su información a través de Internet sin su consentimiento, lo que puede generar una infinidad de sentimientos negativos y traumáticos **(PRC, 2018)**. Dada la importancia actual del tema y la creciente demanda de un marco legal y regulatorio para abordar de manera más efectiva la violencia en línea contra las mujeres, este Libro Blanco tiene como objetivo hacer unos aportes sobre la necesidad de combatir esta violencia. El documento explica brevemente cómo se puede acosar a las mujeres en línea, y describe algunos de los principales problemas en las esferas pública y privada. También revisa brevemente cómo se han abordado estos problemas en los países de América Latina y el Caribe. Por último, presenta un conjunto de herramientas que ofrece pasos prácticos que pueden seguir las mujeres que desean protegerse de los riesgos de ser expuestas en línea.

Violencia en línea contra las mujeres

2

La Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia contra la Mujer de 1994 (Convención de Belém do Pará), define la violencia contra las mujeres como "...cualquier acción o conducta, basada en su género, que cause muerte, daño o sufrimiento físico, sexual o psicológico a la mujer, tanto en el ámbito público como en el privado" (artículo 1).[2] Cuando la Convención fue escrita y adoptada a principios de la década de 1990, la "esfera pública" no incluía el mundo en línea. Sin embargo, la sociedad ha cambiado radicalmente en los últimos 25 años y nuestras identidades, actividades e interacciones en línea son un componente cada vez más importante de nuestra vida pública, especialmente para figuras políticas, periodistas y otras personas que viven la mayoría de sus vidas en la esfera pública. Nuestra actividad en línea también ha contribuido a volver borrosa la línea entre las esferas pública y privada, hasta el punto en que, para algunos, esa distinción ya no tiene utilidad.

El sistema interamericano de derechos humanos aún no ha establecido una definición acordada de la multiplicidad de comportamientos que constituyen la "violencia en línea" contra las mujeres en el marco de los instrumentos legales existentes, como la Convención de Belém do Pará, y existe una necesidad urgente de establecer estos estándares para poder preparar una base conceptual y normativa sólida para las políticas públicas y otras acciones que tengan como objetivo abordar la violencia en línea contra las mujeres.

En términos concretos, la violencia en línea ocurre de diferentes maneras. "Puede significar el envío de correos electrónicos amenazantes o de acoso, mensajes instantáneos o publicación de información en línea" **(RPC, 2018)** y "tiene como blanco a una persona específica, ya sea contactándola directamente o difundiendo información personal suya, causándole angustia, miedo o enojo" **(RPC, 2018)**. Los términos equivalentes que se utilizan son "acoso en línea" y "acoso cibernético". A los fines de este documento, hemos incluido todo tipo de acoso o abuso bajo la expresión más amplia de "violencia en línea contra las mujeres".

El Pew Research Center (2017) describe seis comportamientos diferentes que ha clasificado como "acoso en línea", a saber: "insultos ofensivos"; "vergüenza intencional"; "amenazas físicas"; "acoso sostenido"; "acoso sexual" y "acecho". **Citron (2014)** describe que el "acoso cibernético" ... "implica amenazas de violencia, invasiones de privacidad, mentiras

[2] https://www.oas.org/en/mesecvi/convention.asp

que perjudican la reputación, convocatorias a que extraños físicamente dañen a las víctimas y ataques tecnológicos" (p.3). Las consecuencias de dicho acoso van desde angustia mental, daños en la reputación y miedo a los efectos en el mundo real, y el problema es aún más frecuente entre las mujeres **(Pew Research Center, 2017 e INEGI, 2015)**.

Las redes sociales pueden usarse como una herramienta para el acoso. Un estudio realizado por **Amnistía Internacional (2019)** descubrió que es más probable que se acose y maltrate a las mujeres en Twitter, con "amenazas directas o indirectas de violencia física o sexual, abuso discriminatorio dirigido a uno o más aspectos de la identidad de una mujer, hostigamiento selectivo y violaciones de la privacidad, como doxing, o compartir imágenes sexuales o íntimas de una mujer sin su consentimiento". Si bien los tribunales todavía están tratando de comprender las diferencias a menudo sutiles entre la libertad de expresión/expresión protegida y lo que constituye una "verdadera amenaza" **(Drake, 2015)**, muchas mujeres se están sintiendo inseguras en línea y están sufriendo violaciones de sus derechos humanos de poder vivir sin violencia, a la integridad física, mental y moral, y a la privacidad.

El abuso discriminatorio puede ser peor cuando la mujer pertenece a una población indígena, es una persona en situación de discapacidad o con cualquier otra identidad interseccional. Además, el problema del acoso es cada vez más frecuente si se tiene en cuenta la cantidad de información y datos sobre nosotros que están disponibles en línea, el tiempo que pasamos en línea, así como el hecho de que dependemos de Internet para diferentes tipos de interacciones sociales y profesionales. Con lo anterior, es urgente la necesidad de tener una respuesta inmediata que sea legalmente sólida y técnicamente exigible.

|a. ¿Cuáles son algunos de los métodos utilizados en la violencia en línea?|

• **"Ciberacoso"** *[Cyberbullying]*: El **Centro de Investigación de Ciberacoso**, citando a **Hinduja y Patchin (2014)**, lo define como "daño intencional y repetido infligido mediante el uso de computadoras, teléfonos celulares y otros dispositivos electrónicos", destacando su naturaleza repetitiva. **Ipsos (2018)** descubrió que la conciencia sobre el tema ha aumentado en los últimos años. No obstante, las adolescentes tienen más probabilidades de ser víctimas de acoso cibernético que los adolescentes **(Patchin, 2016)**. Además, **Betts et al. (2017)** encontró un impacto negativo en cómo se percibe el valor del aprendizaje entre las mujeres que están sujetas a la intimidación, lo que no ocurre de manera similar entre los hombres. **Kwon et al. (2019)** descubrieron que ser víctima del acoso cibernético está correlacionado con mala calidad del sueño, lo que aumenta las posibilidades de depresión entre adolescentes.

•"**Ciberacecho**" *[Cyberstalking]:* La organización Privacy Rights Clearinghouse explica que un tipo de acoso en línea es el acecho cibernético, que "implica el uso de medios electrónicos para acechar a una víctima y generalmente se refiere a un patrón de conductas amenazantes o maliciosas" (**PRC, 2018**). Existen diferentes definiciones para el término: en algunos casos la amenaza debe considerarse creíble; y en otros, la categoría incluye una amenaza implícita (**RPC, 2018**). Es relativamente fácil acechar a una persona, considerando que muchos tienen múltiples cuentas de redes sociales y una sustancial presencia en línea. Además, muchas personas no son plenamente conscientes de las características de privacidad ofrecidas por las plataformas utilizadas.

• **"Ciberturbas"** *[Cyber Mobs]:* es un concepto relacionado y ocurre cuando grupos en línea publican contenido ofensivo/destructivo en línea, a menudo compitiendo con otros grupos, con

la intención de avergonzar a alguien (Citron, 2014). **Coding Rights e InternetLab (2017)** presentan un ejemplo de cómo afecta esto a las mujeres: una artista brasileña del estado de Bahía (noreste de Brasil) estaba liderando un concurso en línea cuando se organizó una ciberturba contra ella, en una campaña de votación masiva en pro de su competidor, lo que resultó en que ella obtuviera el segundo lugar en el concurso.

• **"Doxing/Doxxing"**: El vocablo "Dox" proviene de "documentos"/".doc" y doxing es la "recuperación y publicación no autorizadas, a menudo mediante piratería, de la información personal de una persona, incluidos, entre otros, nombres completos, direcciones, números de teléfono, correos electrónicos, nombres de cónyuges e hijos, detalles financieros" **(Women's Media Center, 2019)**. Amnistía Internacional descubrió en 2017 que una cuarta parte de las mujeres han sido sometidas a doxing al menos una vez **(Amnistía Internacional, 2017)**.

• **"Robo de identidad"** *[Identity Theft]:* se produce cuando los datos personales de una persona son utilizados de manera engañosa por otra persona (Women's Media Center, 2019). Por ejemplo, una mujer rusa descubrió que sus fotos estaban siendo utilizadas por otra cuenta de Twitter que se había vuelto viral, y le tomó tiempo poder recuperar completamente su identidad (Kochetkova, 2016). Tal robo de identidad puede tener consecuencias tanto prácticas como psicológicas que duran más de lo que uno podría imaginar.

• "**Porno vengativo"/"Pornografía no consensuada"** *[Revenge Porn/Non-consensual pornography]:* es "la distribución de imágenes sexualmente gráficas de personas sin su consentimiento" y esto incluye imágenes/videos adquiridos con o sin consentimiento **(Netizens, 2019)**. Tales escenarios son particularmente dañinos para las mujeres, dado que sus cuerpos y su sexualidad están sujetos a normas culturales que, en muchos casos, son misóginas. Un concepto relacionado es la "sextorsión", donde se hacen demandas de dinero, u otras, a cambio de no revelar imágenes o videos con contenido sexualmente explícito. Teniendo en cuenta que en algunos países más del 80% de los adultos han enviado mensajes de texto con algún tipo de contenido sexual explícito **(Stasko y Geller, 2015)**, muchas personas están en riesgo de sufrir este tipo de violencia en línea.

CUADRO #1 Ultrafalso *[Deepfake]*: Una nueva arma contra las mujeres

"Deepfakes" son videos que utilizan técnicas de aprendizaje automático para intercambiar la cara de una persona con la de otra **(Knight, 2019)**. Dichas tecnologías surgieron en 2017 **(Deeptrace, 2019**) y se están utilizando en diferentes contextos, pero las más comunes están relacionadas con política y pornografía. La cantidad de videos falsos en línea está creciendo exponencialmente y se debe en parte al hecho de que ahora es más fácil para los no expertos usar ciertas tecnologías **(Deeptrace, 2019)**. El Departamento de Defensa de EE. UU. está desarrollando herramientas para automatizar herramientas forenses con el objetivo de atrapar los *deepfakes* **(Knight, 2019)**.

Según **Deeptrace (2019)**, las mujeres son los principales objetivos cuando se usan *deepfakes* en pornografía. También comienzan a aparecer casos relacionados con el uso de dicha tecnología para atacar a las mujeres en la política. Un ejemplo es una conocida política estadounidense, que en 2019 apareció en un video como si estuviera ebria. El video se volvió viral rápidamente en Facebook **(Rosenberg, 2019)**. Esto es especialmente preocupante dado de que se espera que las *deepfakes* afecten seriamente las próximas elecciones en todo el mundo **(Parkin, 2019**).

Aunque todas las mujeres corren riesgos de ser acosadas en línea, otros aspectos de la identidad, como la raza, el origen étnico, el idioma, la orientación sexual o la identidad de género, el estado migratorio y la discapacidad, entre otros, pueden agravar el problema. Las mujeres que pertenecen a diversas identidades simultáneamente son objetivos más vulnerables para sufrir una violencia en línea. Como explica el Women's Media Center (2019), una mujer homosexual podría sufrir los efectos de homofobia, mientras que una mujer negra puede ser un blanco de racismo, y ambos casos también podrían ser blanco de sexismo. Esto destaca la importancia de ver la violencia en línea contra las mujeres desde una perspectiva interseccional.

Las mujeres que participan en la vida política también son blanco frecuente de hostigadores en línea. La Organización de los Estados Americanos (OEA) adoptó una Declaración sobre la violencia y el acoso político contra las mujeres en 2015, que reconoce los "los factores estructurales que inciden en la violencia contra las mujeres y las normas socio-culturales y simbólicas así como los estereotipos sociales y culturales que la perpetúan" (OEA, 2015). La declaración alienta a las redes sociales, entre otras partes interesadas, a adoptar medidas para eliminar la discriminación y los estereotipos sexistas (OEA, 2015). Esto es de vital importancia dado que los debates políticos ocurren cada vez más a través de las plataformas de redes sociales y muchas personas ahora reciben sus noticias sobre política principalmente a través de tales plataformas.

Al recorrer esta descripción general, es posible concluir que las mujeres están siendo atacadas a través de diversos métodos y tecnologías. A continuación, se presenta una breve descripción de cómo se abordan algunos de estos problemas en los países de América Latina y el Caribe.

¿Cómo se abordan estos problemas en los países de América Latina y el Caribe?

3

Se han visto avances en los últimos años en los países de América Latina y el Caribe en la lucha contra la violencia en línea contra las mujeres. Con respecto a la legislación contra el "porno vengativo", por ejemplo, se promulgó la Ley # 13.772/2018[3] en diciembre de 2018 en Brasil, que modifica la legislación anterior para penalizar la grabación no autorizada y la exposición de contenidos desnudos o sexuales. Dichos actos se están considerando ahora como "violencia doméstica" a los efectos de la ley, en los casos en que hubo una relación preexistente entre la víctima y el autor. Los medios de comunicación tuvieron un papel crucial en el fomento del debate sobre el porno vengativo después de la ocurrencia de casos concretos. Dichos debates llevaron a cambios legislativos que abordan directamente el problema (Neris et al., 2018). Argentina, Chile, México y Uruguay son ejemplos de Estados Miembros de la OEA que actualmente están discutiendo proyectos de ley relacionados con el porno vengativo (Neris et al., 2018). México en particular ha propuesto una enmienda específica a su Código Penal y la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia[4] que aborde el acoso cibernético contra las mujeres. **(Cruz, 2019)**.

Además, varios países de América Latina han aprobado legislación sobre acoso político contra las mujeres (Bolivia) o están discutiendo proyectos de ley relacionados (Costa Rica, Ecuador, Honduras, México y Perú) **(OEA, 2017)**. Según lo descrito anteriormente, esto es crucial, entre otras razones, debido al impacto que tiene la tecnología en los debates democráticos.

En lo que respecta a la policía especializada en ciberdelito y/o violencia en línea contra las mujeres, también se han visto avances en los últimos años. México tiene una división de su servicio policial que se centra específicamente en el delito cibernético, atendiendo casos de violencia en línea[5], además de un portal gubernamental en línea que tiene contenidos específicamente relacionados con la concientización sobre el acoso cibernético[6]. En Brasil, algunos estados tienen departamentos de policía especializados, pero otros no[7]. En Perú, cualquiera puede interponer una denuncia de violencia en línea

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

[4] Ley General de Acceso de las Mujeres a una Vida Libre de Violencia

[5] http://www.ssp.df.gob.mx/ciberdelincuencia.html

[6] https://www.gob.mx/ciberbullying

[7] https://new.safernet.org.br/content/delegacias-cibercrimes

a través de un formulario en línea, incluso si la persona que interpone la denuncia no es la víctima[8].

Esta no es una revisión exhaustiva de lo que está sucediendo en los países de América Latina y el Caribe. Más bien, es una breve descripción destinada a demostrar la complejidad del problema. Es posible notar que los países se están moviendo hacia el reconocimiento y la definición del problema, así como al fortalecimiento de las protecciones para las mujeres en línea. Al mismo tiempo, están apareciendo nuevos métodos y tecnologías, y se están poniendo en práctica varias formas de violencia en línea todos los días.

Con el fin de contribuir a las protecciones vigentes para las mujeres en línea, este Libro Blanco concluye con una serie de pasos prácticos que las mujeres pueden tomar, así como recursos útiles que están disponibles en línea.

[8] http://www.noalacosovirtual.pe/

Pasos prácticos que se pueden tomar de inmediato

4

Comenzar con los pasos prácticos que se detallan a continuación resulta conveniente si usted desea protegerse contra la violencia en línea. También se encuentran contenidos útiles en línea que puede consultar. Entre estos contenidos hay guías y manuales que lo/la ayudarán a comprender mejor qué es la violencia en línea contra las mujeres y qué medidas se pueden tomar contra ella.

|Medidas preventivas:|

• **Utilice contraseñas seguras y no las comparta.** Asegúrese de tener una contraseña segura y de guardársela. Además, no repita las contraseñas por diferentes plataformas y servicios. Para obtener más información, consulte **OEA (2019)** "Contraseñas, qué hacer y qué no hacer" (p. 11).

• **Aprenda a comprender y cambiar la configuración de privacidad de las plataformas de redes sociales.** Parte de la información expuesta en línea se puede controlar a través de la configuración de privacidad. Es importante saber cuáles son las opciones en términos de protección de su privacidad. Por ejemplo, es importante mantener sus mensajes publicados privados para que las personas que están fuera de su red no tengan acceso a los contenidos que publica, y utilizar el sistema de doble verificación para iniciar sesión. Para obtener más información, consulte **OEA (2019)** "Verifique su configuración de privacidad" (p. 09).

• **Use aplicaciones de mensajería cifradas para comunicarse.** Las aplicaciones cifradas son una opción más segura, ya que es más difícil para una persona acceder a los contenidos que se intercambian a través de ellas. Si bien los mensajes de texto normales de teléfonos celulares no están encriptados, las aplicaciones como *Signal, Telegram, WhatsApp* y *Wire* sí lo están.

• **Use una red privada virtual (VPN) para cifrar su tráfico en línea** Este paso es importante especialmente cuando usted no está utilizando una red privada (cuando está accediendo a Internet desde una cafetería u otra red inalámbrica pública, por ejemplo). Los servicios VPN permitirán que su tráfico se cifre para que otras personas que usan la red no puedan ver lo que usted está haciendo en línea. Aunque la mayoría de los servicios de VPN no son gratuitos, son una buena inversión. Para obtener más información, consulte **OEA (2019)** "Uso de VPN" (p. 13).

Si ocurre una violencia/acoso/amenaza/abuso:

• **Guarde la prueba de la violencia/acoso/amenaza/abuso.** No borre ninguna prueba. Es crucial mantener cualquier mensaje que tenga y cualquier otra forma de evidencia, como capturas de pantalla que puedan usarse para probar la violencia/acoso/amenaza/abuso.

• **Denuncie la violencia a la plataforma/servicio en línea.** En la mayoría de los casos, es posible denunciar la violencia a la plataforma/servicio en línea mismo. Informe lo que ha ocurrido de inmediato. La plataforma investigará para determinar si el contenido intercambiado viola los "estándares comunitarios" existentes y podrá o no tomar medidas para eliminar el contenido y/o restringir los privilegios y la actividad del autor. Si bien cada plataforma tiene sus propias reglas, usted puede buscar un ejemplo de cómo se abordan la eliminación de contenido y otros aspectos de la exigibilidad de las reglas en **OEA (2019)** "Exigibilidad de nuestras reglas" (p. 28).

• **No responda a ningún mensaje de amenaza/acoso.** Es importante no "alimentar" a la persona que está cometiendo la violencia. No responda a ningún mensaje que sea intimidante/amenazante. Si es posible, bloquee a la persona para que ya no se puedan recibir mensajes. En la mayoría de los casos, la persona que usted ha bloqueado no recibirá una notificación si la bloqueó.

• **Comuníquese con las autoridades locales [Este paso debe tomarse con precaución ya que solo se deben denunciar las amenazas graves].** Además de las autoridades del orden público regulares, hay autoridades especializadas en muchos países, como la policía especializada en delitos cibernéticos. Comuníquese con ellos o con cualquier otra autoridad local que pueda brindar ayuda. En algunos casos, también hay divisiones policiales especializadas en violencia contra las mujeres, así como formularios en línea que pueden usarse para registrar denuncias de violencia en línea.

• **Busque el apoyo de personas de su confianza y profesionales de salud mental.** Ser víctima de violencia en línea es preocupante y puede afectar profundamente la salud mental y el bienestar de una persona. Es importante contar con el apoyo externo de profesionales y personas de su confianza cercanas. Ellos podrán ayudarla a tomar las medidas adecuadas para abordar el problema.

• **Busque recursos útiles en línea.** Hay manuales, cajas de herramientas y una amplia gama de material en línea que se puede consultar. Algunas de estas herramientas se detallan a continuación en la **Sección 5. "Contenido útil en línea"**. Verifique, además, "Alfabetización mediática y seguridad digital" **(OAS, 2019).**

Contenidos útiles en línea

5

[Informes, Manuales and Cajas de herramientas]

• Alfabetismo y Seguridad Digital. Mejores prácticas en el uso de Twitter. OEA 2019 https://www.oas.org/es/sms/cicte/docs/20190913-DIGITAL-Alfabetismo-y-seguridad-digital-Twitter.pdf

• Acoso Online. Pornografia no consentida. Cinco claves para denunciar y resistir su publicación. 2017. (Spanish) Fundación Datos Protegidos; Equipo Latinoamérico 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. *[Una primera mirada a la seguridad digital. Acceda ahora]* 2018. (English) 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. *[Una caja de herramientas para investigar el acceso y uso de internet por parte de las mujeres]* A4AI; World Wide Web Foundation, GSMA and APC. 2018. (English) 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. *[Promoción de los derechos de las mujeres en línea: brechas y oportunidades en la investigación e incidencia.]* World Wide Web Foundation. 2018. (English) https://webfoundation.org/research/advancing-womens-rights-online-gaps-and-opportunities-in-research-and-advocacy/

• Online Harassment Field Manual. *[Manual de campo sobre el acoso en línea]* PEN America. 2019. (English) https://onlineharassmentfieldmanual.pen.org/

• Manuals with a Gender Perspective. *[Manuales con enfoque de género]* Tactical Tech. (English and Spanish) https://gendersec.tacticaltech.org/wiki/index.php/Manuals_with_a_gender_perspective

• Violencia Cibernetica. Lersy G. Boria Vizacarrondo. Procuradora de las Mujeres, Puerto Rico. (Spanish) http://www.mujer.pr.gov/Educaci%C3%B3nPrevenci%C3%B3n/Opusculos/Violencia%20Cibernetica.pdf

• Netizens Online Security Guide. *[Guía de seguridad en línea para internautas]* 2019. (English) https://drive.google.com/file/d/0B-xwQoatiZyBVTZid3ZrdUk2R28/view

• Safernet. Contenidos acerca del ciberacoso. (Portuguese) https://new.safernet.org.br/

|TEDTalks|

• How Online Abuse of Women Has Spiraled Out of Control. *[Cómo se ha desbocado el abuso en línea contra las mujeres]* Ashley Judd. TEDTalk. 2016 (English). https://www.ted.com/talks/ashley_judd_how_online_abuse_of_women_has_spiraled_out_of_control/transcript?language=en

• Anita Sarkeesian at TEDxWomen 2012. *[Anita Sarkeesian en TEDxWomen 2012]* Anita Sarkeesian. 2012. (English) https://www.youtube.com/watch?v=GZAxwsg9J9Q

• Grooming, el acoso ¿virtual?. Sebastián Bortnik. TEDxRíodelaPlata. 2016. (Spanish) https://www.youtube.com/watch?v=0wZjKOulodo

|Documentales|

• Netizens. *[Internautas]* Cynthia Lowen. 2019. (English) https://www.netizensfilm.com/

Referencias

6

Amnesty International. (2017). Amnistía revela alarmante impacto de los abusos contra las mujeres en Internet. Retrieved from https://www.amnesty.org/es/latest/news/2017/11/amnesty-reveals-alarming-impact-of-online-abuse-against-women/

Amnesty International. (2019). Why Twitter is a toxic place for women. Retrieved from 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. Retrieved from 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. Retrieved from 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. Retrieved November 3, 2019, from Comparitech website: https://www.comparitech.com/internet-providers/cyberbullying-statistics/

Cruz, H. (2019). Proponen ley contra ciberacoso a la mujer. Retrieved November 12, 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? Retrieved November 3, 2019, from Cyberbullying Research Center website: https://cyberbullying.org/what-is-cyberbullying

Deeptrace. (2019). The State of Deepfakes: Landscape, Threats and Impact. Retrieved from 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. Retrieved November 3, 2019, from Pew Research Center website: 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. Retrieved from https://2b37021f-0f4a-4640-8352-0a3c1b7c2aab.filesusr.com/ugd/04bfff_33ded6f6855b4de5b7a09186e1c6add7.pdf

Franceschi-Bicchierai, L. (2017, September 21). This Ransomware Demands Nudes Instead of Bitcoin. Retrieved November 5, 2019, from Vice website: 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? Retrieved November 4, 2019, from InternetLab website: 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. Retrieved from 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. Retrieved from 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. Retrieved from 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. Retrieved from 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. Retrieved from InternetLab website: http://www.internetlab.org.br/wp-content/uploads/2018/05/Neris_Ruiz_e_Valente_Enfrentando1.pdf

Netizens. (2019). Netizens Online Security Guide. Retrieved from https://drive.google.com/file/d/0B-xwQoatiZyBVTZid3ZrdUk2R28/view?usp=embed_facebook

OAS. (2015). Declaration on Political Harassment and Violence Against Women. Retrieved from 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. Retrieved from https://www.oas.org/en/cim/docs/ViolenciaPolitica-FactSheet-ES.pdf

OAS. (2019). Media Literacy and Digital Security: Twitter Best Practices. Retrieved from 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. Retrieved from 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. Retrieved November 3, 2019, from Cyberbullying Research Center website: https://cyberbullying.org/2016-cyberbullying-data

Pew Research Center. (2017). Online Harassment 2017. Retrieved November 12, 2019, from https://www.pewinternet.org/wp-content/uploads/sites/9/2017/07/PI_2017.07.11_Online-Harassment_FINAL.pdf

PRC. (2018). Online Harassment & Cyberstalking. Retrieved November 5, 2019, from Privacy Rights Clearinghouse website: 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. Retrieved from 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. Retrieved November 12, 2019, from 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. Retrieved from 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. Retrieved from 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. Retrieved November 3, 2019, from http://www.womensmediacenter.com/speech-project/online-abuse-101

World Bank. (2019). Population, female (% of total population) | Data. Retrieved October 12, 2019, from https://data.worldbank.org/indicator/SP.POP.TOTL.FE.ZS

OEA Más derechos para más gente

Canadá

COMBATIR LA VIOLENCIA EN LÍNEA CONTRA LAS MUJERES

UN LLAMADO A LA PROTECCIÓN

White paper series

Edición 7

2019