La violencia de género en línea contra las mujeres y niñas

Guía de conceptos básicos

OEA | CICTE

OEA | CIM | MESECVI

Créditos

Luis Almagro
Secretario General
Organización de los Estados Americanos

Arthur Weintraub
Secretario de Seguridad Multidimensional
Organización de los Estados Americanos

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

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

Equipo Técnico de la OEA

Programa de Ciberseguridad
Kerry-Ann Barrett
Mariana Cardona
Gabriela Montes de Oca Fehr

Comisión Interamericana de Mujeres /
Mecanismo de Seguimiento de la Convención de Belém do Pará
Luz Patricia Mejía Guerrero
Alejandra Negrete Morayta

Autora
Katya N. Vera Morales

Diseño y Diagramación
Michelle Felguérez

Con el apoyo financiero del Gobierno de Canadá

OAS Cataloging-in-Publication Data

La violencia de género en línea contra las mujeres y niñas : Guía de conceptos básicos, herramientas de seguridad digital y estrategias de respuesta / [Preparado por la Secretaría General de la Organización de los Estados Americanos].
v. ; cm. (OAS. Documentos oficiales ; OEA/Ser.D/XXV.25)
ISBN 978-0-8270-7306-7
1. Girls--Violence against. 2. Women--Violence against. 3. Computer security. 4. Computer crimes. 5. Girls--Crimes against. 6. Women--Crimes against. I. Title: Guía de conceptos básicos, herramientas de seguridad digital y estrategias de respuesta. II. Inter-American Commission of Women. III. Inter-American Committee against Terrorism. IV. OAS/CICTE Cyber Security Program. V. Organization of American States. Secretariat for Multidimensional Security. VI. Vera Morales, Katya N. VII. Series.
OEA/Ser.D/XXV.25

Índice

Esta publicación se realizó gracias al apoyo brindado por el Departamento de Estado de los Estados Unidos, bajo los términos del Proyecto No. SLMQM20GR2380. Las opiniones expresadas en este documento pertenecen a los autores y no reflejan necesariamente las opiniones del Departamento de Estado de los Estados Unidos.

Introducción

La violencia de género facilitada por las nuevas tecnologías es un fenómeno que de forma creciente afecta la privacidad y seguridad de las mujeres dentro y fuera del ciberespacio. Investigaciones sobre el tema indican que **las mujeres son víctimas de ciertos tipos de ciberviolencia de manera desproporcionada en comparación con los hombres** (REVM-ONU, 2018; EIGE, 2017). De acuerdo con un estudio publicado en 2015 por la Comisión de la Banda Ancha para el Desarrollo Sostenible, de las Naciones Unidas, 73% de las mujeres habían vivido alguna forma de violencia de género en línea, mientras que 61% de los atacantes eran hombres (UNBC, 2015). Otras fuentes señalan que 23% de las mujeres han experimentado acoso en línea al menos una vez en su vida, y se estima que una de cada diez mujeres ya había sufrido alguna forma de ciberviolencia desde los 15 años de edad (REVM-ONU, 2018, párr. 16; EIGE, 2017: 3; AI, 2017).

Además, como lo han comprobado múltiples fuentes[1], esta violencia se ha agravado con las restricciones de la movilidad y el confinamiento impuestos a raíz de la pandemia de COVID-19: a medida que más mujeres y niñas se vuelcan a los espacios digitales, la ciberviolencia de género en su contra se incrementa (ONU Mujeres; CIM, 2020; Derechos Digitales, 2020).

Este fenómeno se observa en un escenario con múltiples retos. La información sobre la ciberviolencia contra las mujeres es aún escasa. Es muy poco lo que se sabe sobre el porcentaje real de víctimas y la prevalencia de los daños que provoca (EIGE, 2017). Además, hasta la fecha no hay una definición acordada a escala regional o internacional de la violencia de género en línea ni una terminología precisa[2]. Hay una gran disparidad entre las respuestas de los Estados y los organismos internacionales y, en general, una falta de marcos jurídicos adecuados para proteger a las víctimas.

Tomando en consideración este contexto, el Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo (CICTE), en alianza con la Comisión Interamericana de Mujeres (CIM), ha elaborado esta guía de conceptos básicos dirigida a instituciones públicas, profesionales y partes interesadas en el sector de la ciberseguridad. En ella se abordan las características y el impacto de la violencia de género en línea (primera parte), los tipos de ataques que pueden ser considerados como manifestaciones de violencia de género digital (segunda parte), y se presenta una breve reseña de los últimos desarrollos en la materia en la región latinoamericana y de las medidas que pueden adoptar las autoridades para prevenir y combatir esta forma de violencia de género (tercera parte).

Esta guía forma parte de la publicación *La violencia de género en línea contra las mujeres y niñas. Guía de conceptos básicos, herramientas de seguridad digital y estrategias de respuesta*, en la cual se encontrará mayor información acerca de las medidas preventivas y herramientas la seguridad digital que pueden adoptarse frente a agresiones y actos de violencia de género en línea.

[1] Unión Internacional de Telecomunicaciones (2019). *Measuring digital development. Facts and figures 2019*. ITU Publications. Disponible en: https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf

[2] Organización Mundial de la Salud. "La violencia contra la mujer es omnipresente y devastadora: la sufren una de cada tres mujeres". Disponible en: https://www.who.int/es/news/item/09-03-2021-devastatingly-pervasive-1-in-3-women-globally-experience-violence

Parte uno

Conceptos básicos:

RECONOCER LA VIOLENCIA DIGITAL ES EL PRIMER PASO PARA COMBATIRLA

A

¿Qué es la violencia de género en línea contra mujeres y niñas?

Elementos básicos de la violencia en línea en contra de las mujeres:

01 No es algo nuevo. Forma parte de un contexto de discriminación de género y violencia sistémica contra las mujeres que se da en todos los ámbitos de su vida.

02 No está desconectada de la violencia "fuera de internet": es parte de la serie de formas múltiples, interrelacionadas y recurrentes de violencia contra las mujeres y las niñas que ahora fluye por el mundo *online-offline* y lo atraviesa.

03 Conlleva diversas violaciones de los derechos humanos de las mujeres y las niñas.

04 Es una expresión dinámica que abarca prácticas muy diversas de violencia facilitadas o reconfiguradas por las tecnologías de la información y las comunicaciones (TIC).

05 Causa en las víctimas daños y sufrimientos psicológicos, físicos, sexuales y/o económicos, y tiene efectos familiares, sociales y colectivos.

La violencia en línea contra las mujeres no es un fenómeno aislado, sino que **se localiza en un contexto social más amplio de desigualdad y discriminación de género contra las mujeres y las niñas.** Por ello, para entender la violencia digital, es crucial que nos detengamos primero a analizar qué es la violencia de género, puesto que las agresiones y los ataques que viven las mujeres en sus interacciones en línea no son más que una extensión de la violencia que por muchos años las ha afectado en todas las esferas de su vida.

¿Qué es la violencia de género contra las mujeres y las niñas?

De acuerdo con la Convención de Belém do Pará, se entiende como violencia contra la mujer "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).

La violencia por razón de género es **"la violencia dirigida contra la mujer porque es mujer o que la afecta en forma desproporcionada"** (Comité CEDAW, Recomendación General 19, párr. 6).

La violencia de género contra las mujeres tiene su origen en estereotipos y prejuicios acerca de los atributos y las características que poseen hombres y mujeres y en expectativas de las funciones sociales que ambos supuestamente deben desempeñar (por ejemplo, que las mujeres son las únicas encargadas de las labores domésticas, que no tienen suficiente autoridad para ocupar cargos directivos o que son débiles por naturaleza). Estos patrones socioculturales colocan a las mujeres en una **posición inferior o subordinada respecto de los hombres** y propician su discriminación, elementos que son los principales impulsores de la violencia dirigida hacia ellas (MESECVI, 2017, párr. 37).

Es importante subrayar que la violencia opera en sinergia con la desigualdad de género y no solo como una consecuencia de ésta última, sino como mecanismo social que busca mantener a las mujeres en una situación de desventaja. Esto significa que la violencia se usa en muchos casos para "castigar" o "corregir" a mujeres cuyas actitudes o actividades supuestamente van en contra de lo que la sociedad espera de ellas (MESECVI, 2017, párr. 36).

Las Naciones Unidas han señalado que la violencia contra las mujeres es un problema omnipresente en todos los países del mundo y una violación sistemática y generalizada de los derechos humanos, con alto grado de impunidad.

Las mujeres y las niñas experimentan violencia de género a lo largo de los años en todos los espacios *offline y online* donde concurren y participan, ya sea en el hogar, la escuela, el trabajo, la vía pública, la política, los medios de comunicación, el deporte, las instituciones públicas o al navegar en redes sociales (Comité CEDAW, Recomendación General 35). Esta violencia no tiene fronteras, está dirigida contra todas las mujeres por el simple hecho de que son mujeres e **incide más en ciertos grupos de mujeres debido a que sufren formas de discriminación interseccional**, como es el caso de las mujeres indígenas, migrantes, con discapacidad, lesbianas, bisexuales y transgénero, entre otras (MESECVI, 2017).

Uno de los logros más importantes para las mujeres ha sido el reconocimiento de que **la violencia cometida en su contra no es un problema privado**, sino que constituye un asunto de interés público y una violación de los derechos humanos reconocida en instrumentos internacionales y legislaciones nacionales que prescriben la obligación de los Estados de prevenirla, atenderla, investigarla, repararla y sancionarla (Edwards, 2010). En el caso del sistema interamericano, el derecho de las mujeres a vivir una vida libre de violencia está reconocido en la Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia contra la Mujer (Convención de Belém do Pará), el primer tratado en la materia que elevó el combate de la violencia de género contra las mujeres al rubro de problema de interés regional[3].

¿Qué es la violencia de género en línea contra las mujeres?

Si bien varias organizaciones de la sociedad civil, el sector académico y organismos internacionales han realizado esfuerzos importantes para precisar qué es la violencia de género en línea en contra de las mujeres, como se señaló al inicio, hasta la fecha no se ha alcanzado un consenso en torno a su definición ni existe una terminología consolidada (Van Der Wilk, 2018).

En 2015, la Asociación para el Progreso de las Comunicaciones (APC), que ha trabajado en este asunto por más de diez años, definió la violencia en línea contra las mujeres como los **actos de violencia por razones de género que son cometidos, instigados o agravados, en parte o en su totalidad, por el uso de tecnologías de la información y las comunicaciones** (TIC), como teléfonos móviles, internet, plataformas de redes sociales y correo electrónico (APC, 2017: 3). Además, el Proyecto de Debida Diligencia (*Due Diligence* Project) destacó que estos actos tienen o pueden tener como resultado un daño o sufrimiento físico, sexual, psicológico o económico (Abdul, 2017).

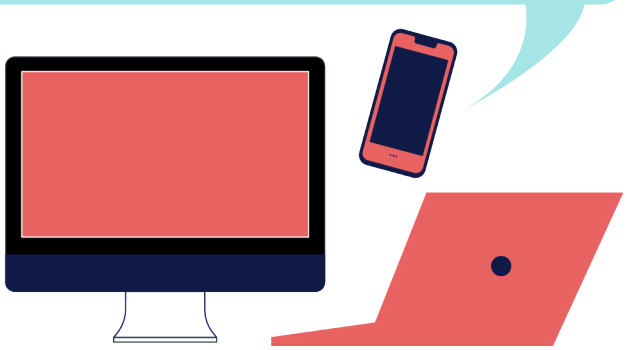
El Centro Internacional de Investigaciones sobre la Mujer, por su parte, define la violencia de género facilitada por las tecnologías como actos de una o más personas que **dañan a otras por razón de su identidad sexual o de género o al imponer normas dañinas de género.** Estos actos, para los cuales se usan la internet o la tecnología móvil, consisten en hostigamiento, intimidación, acoso sexual, difamación, discurso de odio y explotación (Hinson et al., 2018: 1).

Finalmente, en el ámbito de la Organización de las Naciones Unidas (ONU), la Relatora Especial sobre la Violencia contra las Mujeres definió en 2018 la violencia en línea contra las mujeres como "todo acto de violencia por razón de género contra la mujer **cometido, con la asistencia, en parte o en su totalidad, del uso de las TIC, o agravado por este,** como los teléfonos móviles y los teléfonos inteligentes, Internet, plataformas de medios sociales o correo electrónico, **dirigida contra una mujer porque es mujer o que la afecta en forma desproporcionada"** (REVM-ONU, 2018, párr. 23).

[3] Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia contra la Mujer. Disponible en: https://www.oas.org/juridico/spanish/tratados/a-61.html

Los datos y estudios pertinentes han demostrado que, en la mayoría de los casos, la violencia en línea no es un delito neutro en cuanto al género (REVM-ONU, 2018).

La violencia en línea contra las mujeres puede estar facilitada por algoritmos y dispositivos tecnológicos tales como teléfonos móviles e inteligentes, tabletas, computadoras, sistemas de geolocalización, dispositivos de audio, cámaras o asistentes virtuales.



Esta violencia puede verificarse en una gran variedad de plataformas de internet; por ejemplo, redes sociales (*Facebook, Twitter, Tik Tok*), servicios de correo electrónico, aplicaciones de mensajería instantánea (*WhatsApp*), aplicaciones para citas (*Tinder, Grindr, Hinge, Match.com*), videojuegos en línea, sitios donde se intercambia contenido (*Reddit*), foros de discusión en línea (en las secciones de comentarios de los periódicos) o plataformas generadas por los usuarios (blogs, sitios para intercambio de imágenes y videos).

La ciberviolencia de género es un concepto en constante cambio. Como lo reconoció la Relatora Especial sobre Violencia contra las Mujeres de las Naciones Unidas, las rápidas transformaciones tecnológicas influyen en la violencia en línea, y surgen nuevas y diferentes manifestaciones de violencia a medida que los espacios digitales se transforman y trastocan la vida fuera de internet (REVM-ONU, 2018, párr. 24).

La violencia en línea ha variado desde los orígenes de la internet, y seguramente seguirá transformándose a medida que las plataformas digitales y las herramientas tecnológicas sigan avanzando e interrelacionándose más y más en nuestra vida.

El proceso continuo online-offline de la violencia: nuevas formas de la misma violencia

La violencia en línea se manifiesta en una serie de formas múltiples, recurrentes e interrelacionadas de violencia por razón de género contra las mujeres (REVM-ONU, 2018).

No debemos caer en el error de considerar que la violencia en línea es un fenómeno separado de la violencia en el mundo "real", pues forma parte de las manifestaciones continuas e interconectadas de violencia que las mujeres ya vivían fuera de internet.

Estamos hablando de un viejo sistema de dominación y violencia de género que ahora usa una nueva plataforma para replicarse.

En 1989, Liz Kelly llamó la atención por primera vez sobre el hecho de que los diferentes tipos de violencia y abuso de género pueden ser conceptualizados como un **proceso continuo de violencia (*continuum* de violencia) en la vida y las experiencias de las mujeres en todo el mundo** (y no solo como sucesos esporádicos o anormales), que abarca desde actos expresamente reconocidos como delitos hasta conductas de control y dominación tan comunes que han llegado a normalizarse (Kelly, 1989).

Todos los tipos de violencia de género contra las mujeres tienen algo en común: son formas de coerción, abuso o agresión que se usan para controlar, limitar o constreñir la vida, el estatus, los movimientos y las oportunidades de las mujeres y para facilitar y asegurar los privilegios de los hombres (Kelly, 1989).

Por lo tanto, en el contexto actual, en el cual el ciberespacio y la vida fuera de internet están cada vez más interrelacionados, la violencia contra las mujeres ha llegado al mundo digital como una extensión más de esa serie continua de sucesos de violencia que se presentan en la experiencia diaria de mujeres y niñas (Kelly, 1988; Powell, Henry y Flynn, 2018).

Así observamos que, en la era digital, las formas de violencia de género persisten o se amplifican con el uso de nuevas tecnologías y que están surgiendo nuevas formas de sexismo y misoginia en línea, las cuales pueden salir del ciberespacio para convertirse en agresiones físicas contra las mujeres. La violencia contra las mujeres puede, por ejemplo, comenzar como acoso sexual en la vía pública, como violencia "por motivos de honor" en una comunidad o como agresiones físicas perpetradas por una pareja sentimental y convertirse y reubicarse por medio de la tecnología en la distribución no consensuada de imágenes íntimas, en actos de ciberacoso, en discurso de odio sexista en redes sociales, en el monitoreo por medio del celular, etc. En sentido inverso, la violencia puede comenzar como intercambios en las redes sociales por una menor de edad con supuestos nuevos amigos y culminar en encuentros donde se cometen actos de violencia sexual o secuestros. Todos estos actos nuevos inciden en la interacción de las mujeres no solo en línea sino en todos los espacios de su vida *offline*.

En muchos casos, la violencia de género se ha intensificado dado que los espacios digitales ofrecen una muy conveniente anonimidad y el abuso puede cometerse desde cualquier lugar, a través de una amplia gama de nuevas tecnologías y plataformas que los perpetradores de violencia tienen a su alcance y con una rápida propagación y permanencia del contenido digital.

Algunos aspectos de las nuevas TIC que han contribuido a la transformación de la violencia de género contra las mujeres son su rápida expansión, la permanencia en línea de contenidos que dejan un registro digital indeleble, su replicabilidad y alcance global, y la posibilidad de localizar fácilmente a personas e información sobre ellas, lo cual facilita el contacto de los agresores con las víctimas y su victimización secundaria (REVM-ONU, 2018).

Bajo la lupa:

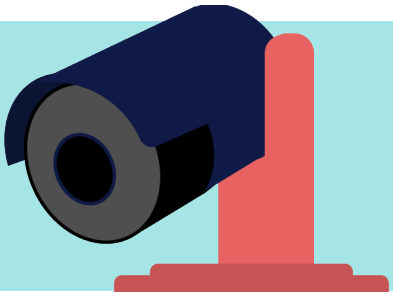
La estrecha relación entre la violencia de pareja y las nuevas tecnologías

Desde hace varios años, las TIC están desempeñando un papel muy importante en el surgimiento de nuevas estrategias de abuso y control por los perpetradores de actos de violencia doméstica y de pareja (Dragiewicz, 2019). Varios estudios han revelado que **77% de las víctimas de ciberacoso han sufrido también alguna forma de violencia física o sexual a manos de una pareja íntima** (FRA, 2014) y que conocían por lo menos a la mitad de los agresores en línea (APC, 2015).

A medida que las nuevas tecnologías se han ido incorporando en prácticamente todas las actividades diarias de las personas, los agresores se han aprovechado, extendiendo e intensificando comportamientos abusivos, posesivos y controladores que antes no eran posibles (Woodlock, 2017). En consecuencia, las mujeres ahora experimentan esta violencia sin límites de espacio y tiempo y con la sensación de que el agresor es omnipresente (Harris, 2018), lo cual tiene efectos graves en su salud mental[4].

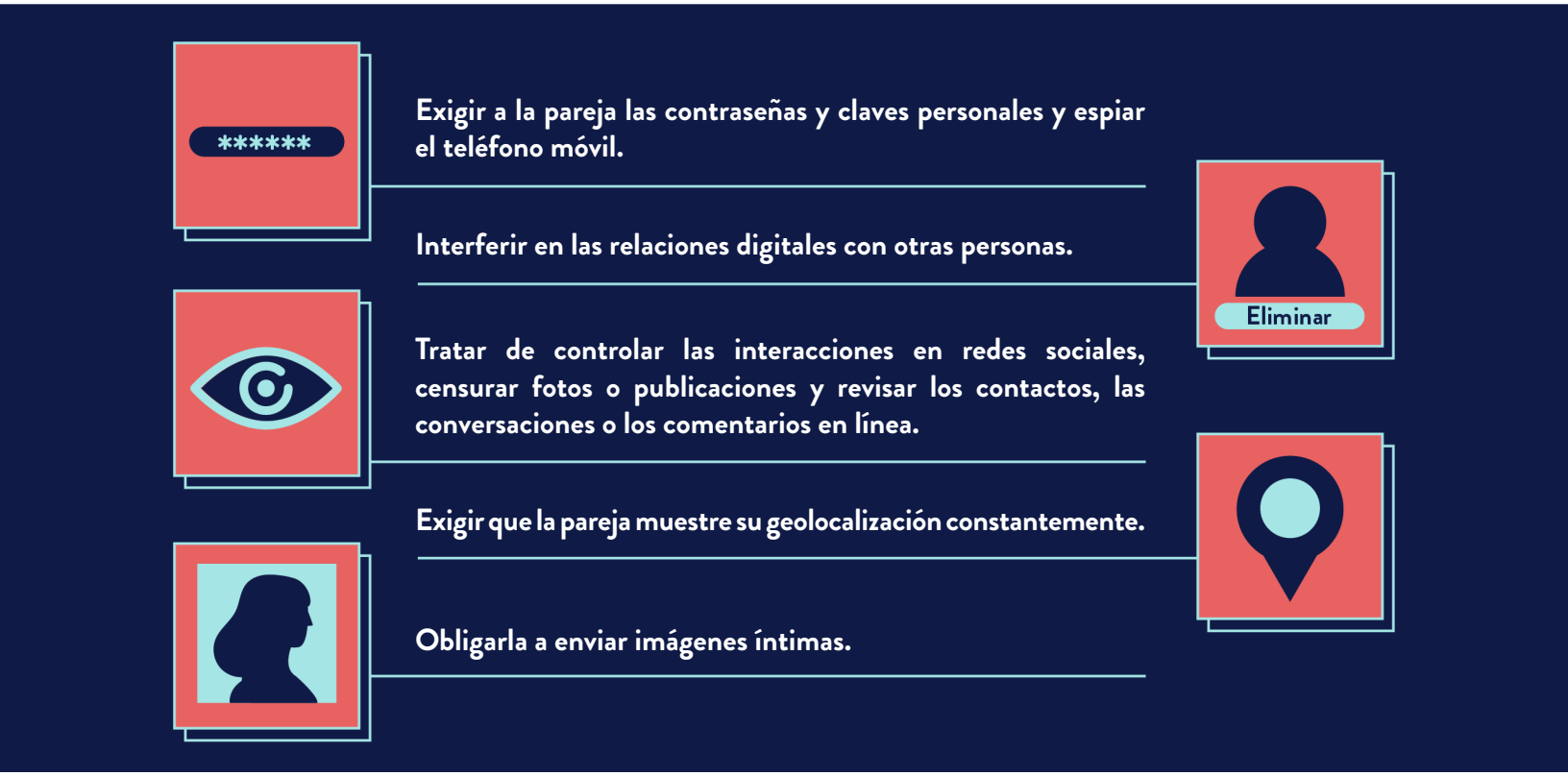
Aunque la investigación en la materia es aún incipiente, varios estudios iniciales indican que algunas tecnologías se usan más que otras para cometer abusos y ejercer cibercontrol en contextos de violencia doméstica o de pareja. Ese es el caso de los mensajes de texto, redes sociales o software para monitorear la ubicación de las víctimas por medio de sus celulares (Dragiewicz, 2019).

No obstante, las manifestaciones del abuso y la vigilancia digital de las mujeres y de la intrusión en su vida cambian constantemente y abarcan desde incidentes de robo de identidad por la pareja o expareja para hacer compras por internet hasta el uso por los agresores de dispositivos inteligentes instalados en los hogares, como termostatos, cámaras, micrófonos, bocinas o cerraduras, para generar estrés psicológico en las víctimas.



[4] Alexandra Topping (2013). "How domestic violence spreads online: I felt he was watching me". *The Guardian*. Disponible en: https://www.theguardian.com/society/2013/sep/03/domestic-violence-spreads-online-watching

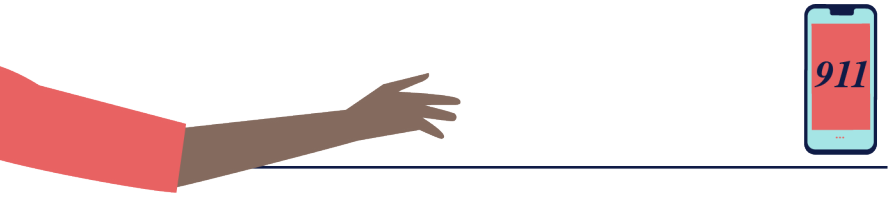
Se ha observado también en parejas jóvenes **nuevos comportamientos que se han normalizado en el actual contexto *online-offline*, disfrazados con ideas y mitos del amor romántico, pero que en el fondo buscan el cibercontrol** y la limitación de la vida digital de las mujeres. Algunos de ellos son los siguientes:



En el caso específico de las víctimas de violencia doméstica y de pareja, la violencia en línea puede disuadirlas de abandonar la relación, dado que muchas veces se sienten atrapadas en una situación de la cual no pueden escapar. Se ha documentado también que, en muchos casos, la violencia digital aumenta en el momento de la separación (no solo contra las víctimas sino también contra sus hijas o hijos, familiares, amistades o parejas sentimentales). Parecería incluso que cortar abruptamente toda comunicación o interacción digital con cierto tipo de agresores puede incrementar el riesgo para las sobrevivientes y su familia (Dragiewicz, 2019).

A esto se suma el **aumento exponencial en todo el mundo de la violencia física y el abuso sexual contra mujeres y niñas durante la pandemia de COVID-19** (ONU Mujeres, CIM, 2019). Con las medidas de confinamiento, se han visto obligadas a permanecer encerradas con sus agresores, y para ellas la tecnología se ha convertido en una herramienta indispensable para comunicarse con el exterior, pedir ayuda y tener acceso a los servicios de atención.

En este contexto, apoyar a víctimas y sobrevivientes de violencia doméstica y de pareja para que sepan reconocer el cibercontrol, proteger su seguridad e integridad digital y **utilizar la tecnología como un medio de apoyo para salir del círculo de violencia** es algo esencial que ahora debe formar parte de los modelos ecológicos de prevención, atención y sanción de la violencia contra las mujeres, que implican un trabajo con familias, comunidades e instituciones.

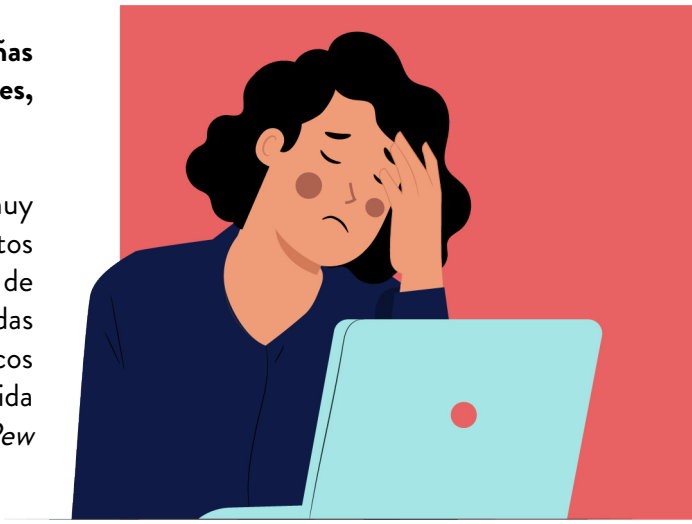


B

¿Qué consecuencias sufren las mujeres y las niñas que son víctimas de violencia en línea?

La violencia en línea contra las mujeres produce daños reales

Como consecuencia de la violencia en línea, las mujeres y las niñas sufren graves daños psicológicos, físicos, sexuales, emocionales, económicos, laborales, familiares y sociales (REVM-ONU, 2018).



Las manifestaciones y las repercusiones de esta violencia pueden ser muy variadas dependiendo de la forma que tome; por ejemplo, sentimientos de depresión, ansiedad, estrés, miedo o ataques de pánico en casos de ciberhostigamiento, intentos de suicidio por parte de mujeres afectadas por la distribución no consensuada de imágenes sexuales, daños físicos contra las víctimas de *doxxing*[5] o perjuicios económicos ante la pérdida del empleo como consecuencia de actos en línea que desprestigian (*Pew Research Center*, 2017; Kwon et al., 2019; AI, 2017).

Se ha comprobado que, como parte del proceso continuo de violencias de género, los daños causados por actos en línea no difieren de los efectos que tiene la violencia fuera de internet, sino que inciden a corto y a largo plazo en todos los ámbitos del desarrollo individual de las mujeres, como su autonomía, privacidad, confianza e integridad (Van Der Wilk, 2018).

Desafortunadamente, persiste una comprensión inadecuada de la seriedad de las consecuencias y los daños que la violencia en línea causa en las mujeres, daños que muchas veces se considera que "no son reales" porque se verificaron en internet. Esto refleja un entendimiento erróneo del proceso continuo *online-offline* en que ahora se desarrolla nuestra vida, así como de las características de la serie de formas múltiples e interrelacionadas de violencias que viven mujeres y niñas en sus interacciones sociales.

[5] *Doxxing* o doxing es un ciberataque que consiste en obtener información personal sobre alguien y hacerla pública en línea.

Se ha observado además que **las características de ciertas tecnologías hacen que la magnitud del daño de algunos actos de violencia se incremente exponencialmente** y se extienda más allá del acto original (como su rápida propagación, alcance, anonimidad y permanencia) (APC, 2017), dado que las mujeres son juzgadas con mayor severidad que los hombres por sus actitudes en línea. Tal es el caso de incidentes de distribución no consentida de imágenes sexuales, en los que se ha visto que mujeres y niñas son estigmatizadas por el ejercicio de su sexualidad y, después de ver sus imágenes distribuidas, tienen que vivir en un contexto de humillación y vergüenza permanente en su entorno social, lo cual en muchos casos las ha empujado al suicidio.

Las mujeres afectadas a menudo se responsabilizan a sí mismas por acciones que pudieran haber causado la violencia y se retiran de los espacios digitales, se autocensuran o se aíslan socialmente (Citron, 2014). Además, es muy común que sean revictimizadas por familiares, autoridades y medios de comunicación, que con frecuencia les atribuyen la responsabilidad de protegerse, en vez de recalcar la conducta ilícita de los agresores, y de esta forma normalizan y minimizan esta violencia (REVM-ONU, 2018, párr. 25).

Aunado a los efectos individuales, **la violencia en línea conlleva daños colectivos e intergeneracionales** y tiene costos directos e indirectos para las sociedades y las economías, dado que las víctimas y sobrevivientes no solo requieren atención médica y servicios judiciales y sociales, sino que también pueden ver disminuida su productividad y sus interacciones en la comunidad (UNBC, 2015). Asimismo, **esta violencia tiene un efecto silenciador**, puesto que es una amenaza directa a la libertad de expresión de las mujeres (AI, 2017) y afecta su acceso y participación en línea como ciudadanas digitales activas, lo cual crea un déficit democrático al impedir que las voces de las mujeres se escuchen libremente en los debates digitales (REVM-ONU, 2018, párr. 29).

Las investigaciones en la materia indican que 28% de las mujeres que fueron objeto de violencia perpetrada por medio de las TIC han reducido deliberadamente su presencia en línea (REVM-ONU, 2018, párr. 26) y se autocensuran por temor a que su privacidad o su seguridad se vean vulneradas (AI, 2017). Para peor, a las sobrevivientes con frecuencia les aconsejan "alejarse" o "retirarse" de las tecnologías tras un incidente de violencia.

Por último, tampoco debemos olvidar que esta violencia **contribuye a la perpetuación de estereotipos de género nocivos y a la reproducción de la violencia sistémica** en el nuevo mundo *online-offline*, al propiciar el desarrollo de tecnologías con sesgos de género.

¿Hay mujeres que están siendo atacadas en línea más que otras?

Al analizar la violencia digital es importante no caer en generalizaciones a partir de una supuesta experiencia común de las mujeres. En cada caso deben tomarse en cuenta las especificidades de las distintas experiencias en línea vividas por las mujeres y las diversas identidades partir de las cuales se definen.

Si bien la violencia en línea es un fenómeno común entre mujeres y niñas que navegan el mundo digital, lo cierto es que también **afecta a las mujeres de forma diferente dependiendo de otras formas de discriminación** que enfrentan en su vida cotidiana por motivos de raza, origen étnico, orientación sexual, identidad de género, clase social o nacionalidad.

Según Amnistía Internacional, las mujeres que enfrentan discriminación fuera de internet debido a rasgos específicos de su identidad con frecuencia encuentran que la violencia y el abuso en línea contra ellas están dirigidos a esos mismos rasgos (AI, 2018). Estas mujeres son particularmente vulnerables a la victimización mediante una combinación de abusos que reflejan creencias racistas, sexistas, estereotipos, prejuicios sociales e ideas sobre un supuesto orden de género.

Asimismo, la Relatora Especial sobre Violencia de Naciones Unidas señaló en su informe de 2018 que ciertos grupos de mujeres son especialmente objeto de violencia en línea, como las parlamentarias, las periodistas, las mujeres jóvenes o que tienen una participación en el debate digital y las mujeres de minorías étnicas o de la comunidad LGBTIQ+ (REVM-ONU, 2018; Van Der Wilk, 2018; UNBC, 2015; EIGE, 2017; Henry y Powell, 2016). Por lo general, la violencia digital contra ellas toma la forma de ataques a su visibilidad, a su sexualidad, a su libertad de expresión y a su participación política. Es evidente que uno de los objetivos de la violencia digital es mantener a las mujeres en silencio y en condiciones de subordinación en la sociedad.

¿Sabías que...?

En varios informes se señala que las mujeres de 18 a 24 años se encuentran en particular riesgo de violencia digital, con una probabilidad 27% mayor de ser víctimas de ciberabuso en comparación con los hombres (APC, 2001; UNBC, 2015). El *Pew Research Center* informó también que estas mujeres son particularmente vulnerables al ciberacoso (*Pew Reserach Center*, 2014 y 2017).

Se ha observado que el simple hecho de ser mujer y ser una figura pública o participar en la vida política conlleva ser blanco de comentarios extremadamente misóginos, violencia sexual y amenazas de violencia física y femicida en línea (Rawlison, 2018). Las mujeres que participan en debates públicos en internet o que escriben sobre temas de género son, de manera desproporcionada, víctimas de acoso en línea con el fin de silenciarlas e intimidarlas y suelen ser el blanco de campañas masivas de abuso y violencia verbal sexualizada, con discurso de odio y amenazas de abuso y violación sexual (REVM-ONU, 2018, párr. 25). De acuerdo con Amnistía Internacional, 88% de las mujeres sufren abusos y ciberacoso tras la publicación de contenidos feministas (AI, 2018).

Bajo la lupa:
mujeres propensas a ser el blanco de ciertos tipos de violencia digital[6]

Mujeres en una relación íntima o víctimas de violencia doméstica o de pareja.

Defensoras de derechos humanos, periodistas, mujeres que participan en actividades políticas, participantes activas en el debate digital o mujeres que tienen un perfil público.
Estas mujeres son frecuentemente objeto de ciberacoso y ciberhostigamiento en internet, incluso de amenazas en línea y abuso verbal de naturaleza misógina y sexual.

Mujeres lesbianas, bisexuales, transgénero o intersex, mujeres con discapacidad, mujeres de una minoría étnica o racial, mujeres indígenas o de grupos marginados. Estas mujeres suelen ser blanco de discurso de odio y abuso en línea con connotaciones homofóbicas, racistas o sexistas.

Las mujeres jóvenes son también un blanco frecuente de violencia sexual en línea, que reproduce formas de hostigamiento, acoso y abuso sexual.

[6] Association for Progressive Communications (APC). *From impunity to justice. Exploring corporate and legal remedies for technology-related violence against women 2012-2015.* Disponible en: https://genderit.org/onlinevaw/

¿Quiénes son los agresores?

Se ha observado que los agresores y los responsables de la violencia de género en línea contra las mujeres tienen por lo general una identidad masculina (Van Der Wilk, 2018, 34-37). Estos agresores pueden ser una persona que la víctima no conoce (como un acosador sexual en línea que dirige sus ataques sistemáticamente hacia diversas mujeres o sujetos que practican el *grooming* o ciberengaño pederasta)[7] o un integrante del círculo familiar, profesional o una amistad. Algunos estudios indican, por ejemplo, que entre **40% y 50% de las víctimas conocían a sus agresores en línea** (una expareja sentimental, un miembro de la familia, un amigo o un colega) y que, **en un tercio de los casos, los agresores tenían o habían tenido una relación íntima con la persona atacada** (*Pew Research Center*, 2017; APC, 2015).

Pueden identificarse dos tipos de responsables de la violencia en línea contra las mujeres (Abdul, 2017):

El perpetrador original:
La persona que comete el acto inicial de violencia o abuso digital o que crea, manipula o publica por primera vez información dañina, datos personales o imágenes íntimas sin el consentimiento de la víctima.

El perpetrador o los perpetradores secundarios:
Persona o grupo de personas que participan en la continuación y propagación de un acto de violencia en línea al reenviar, descargar, volver a publicar o compartir información dañina, datos personales o imágenes íntimas obtenidas sin el consentimiento de la víctima.

¿Qué buscan los agresores con la violencia en línea contra las mujeres y las niñas?
El objetivo de la violencia es crear un ambiente hostil en línea para las mujeres a fin de avergonzarlas, intimidarlas, denigrarlas, menospreciarlas o silenciarlas por medio de la vigilancia, el robo o la manipulación de información o el control de sus canales de comunicación (AI, 2018).

Bajo la lupa:
La violencia en línea como violación de los derechos humanos de las mujeres

Como subraya la Relatora Especial sobre la Violencia contra la Mujer de las Naciones Unidas en su informe de 2018, los derechos humanos de las mujeres amparados por tratados internacionales deben estar protegidos en internet, "en particular mediante la prohibición de la violencia por razón de género en formas facilitadas por las TIC y en línea" (REVM-ONU, 2018, párr. 17).

[7] El *grooming* o ciberengaño pederasta consiste en actos deliberados de un adulto para acercarse a un menor a fin de establecer una relación y un control emocional que le permita cometer abusos sexuales, entablar relaciones virtuales, obtener pornografía infantil o practicar la trata de menores.

Por su parte, el Consejo de Derechos Humanos de las Naciones Unidas reconoció que la violencia en contextos digitales impide "a las mujeres y las niñas disfrutar plenamente de sus derechos humanos y libertades fundamentales" reconocidos en el derecho internacional, lo que obstaculiza su participación plena y efectiva en los asuntos económicos, sociales, culturales y políticos (HRC, 2018, párr. 3).

Algunos de los derechos humanos de las mujeres que la violencia en línea puede violar son los siguientes (REVM-ONU, 2018; Vela y Smith, 2016; APC, 2017):

- **Derecho a la igualdad y no discriminación.**
- **Derecho a una vida libre de violencia.**
- **Derecho a la integridad personal.**
- **Derecho a la autodeterminación.**
- **Derecho a la libertad de expresión, al acceso a la información y al acceso efectivo a internet.**
- **Derecho a la libertad de reunión y asociación.**
- **Derecho a la privacidad y a la protección de los datos personales.**
- **Derecho a la protección del honor y la reputación.**
- **Derechos sexuales y reproductivos de las mujeres.**

Es importante tener presente que "la prohibición de la violencia de género se ha reconocido como un principio del derecho internacional de los derechos humanos" (REVM-ONU, 2018, párr. 17). Eso implica que los Estados tienen obligaciones de debida diligencia de prevenir y combatir la violencia en línea contra las mujeres cometida tanto por agentes estatales como por agentes no estatales (Abdul, 2017).

Bajo la lupa:

El Internet de las Cosas (IoT) y la violencia doméstica

El Internet de las Cosas (*Internet of Things* o IoT por sus siglas en inglés) se refiere a la red de dispositivos inteligentes conectados a internet que pueden compartir datos entre sí. El IoT va más allá de la conectividad entre computadoras, teléfonos celulares y tabletas, e incluye dispositivos como televisiones, relojes, frigoríficos, sistemas de calefacción, cámaras o cerraduras inteligentes.

Se dice que estos dispositivos son "inteligentes" porque pueden recolectar y analizar datos, comunicarse entre ellos y ejecutar acciones sin intervención humana directa. Por ejemplo, por medio del IoT se puede controlar el sistema de seguridad de una casa desde una aplicación instalada en el teléfono celular, mediante comandos de voz dirigidos a asistentes virtuales, o se pueden activar o desactivar remotamente cámaras o sistemas de iluminación.

El IoT tiene muchos beneficios al facilitar cuestiones prácticas de la vida cotidiana, pero puede conllevar potenciales riesgos para la privacidad y la seguridad porque los dispositivos asumen que todas las personas usuarias confían entre sí. Por ejemplo, en el caso de violencia doméstica, un agresor puede utilizar el IoT para monitorear a una víctima o impedirle abrir las cerraduras de su casa, o un *hacker* puede controlar de forma remota una cámara de seguridad para grabar sin consentimiento imágenes o videos íntimos directamente en el hogar de una víctima.

De acuerdo con el proyecto de investigación "Género e Internet de las Cosas" *(Gender and Internet of Things)* de *University College London* (UCL), el IoT facilita tres formas de violencia en línea:

- Ciberhostigamiento.
- Comportamientos coactivos y controladores, incluyendo amenazas de daño o abuso para atemorizar a una víctima. Por ejemplo, denegando el control de la calefacción, la iluminación o de las cerraduras de la casa.
- *Gaslighting* digital, que es una forma de abuso psicológico realizado mediante la manipulación de la realidad de la víctima, con lo cual se busca que se cuestione su cordura, su memoria o su percepción.

Cómo puede afectar el IoT a víctimas de violencia doméstica y violencia sexual

Implicación:
Los perpetradores pueden explotar las funcionalidades del IoT para monitorear, controlar y / o prevenir que las víctimas usen dispositivos.

Consideración:
Es imporante que los servicios de apoyo sean conscientes de las funcionalidades del IoT, dado que pueden informar sobre las evaluaciones y la planificación de la seguridad de las víctimas.

Mitigación:
No existe una estrategia de mitigación única para todos cuando se produce el abuso de tecnología habilitada por IoT. Conocer sus funcionalidades comunes puede ayudar a la hora de buscar el apoyo de profesionales como la policía.

Información:
Dado que los dispositivos de IoT y sus funcionalidades evolucionan constantemente, en el sitio web de STEaPP se proporcionan más recursos e información actualizada sobre el tema.

Fuente: UCL, Gender and IOT Project, *How internet-connected devices can affect victims of gender-based domestic and sexual violence and abuse.* Disponible en: https://www.ucl.ac.uk/steapp/research/digital-technologies-policy-laboratory/gender-and-iot

Parte dos

UN RECORRIDO POR LOS TIPOS

DE VIOLENCIA DE GÉNERO

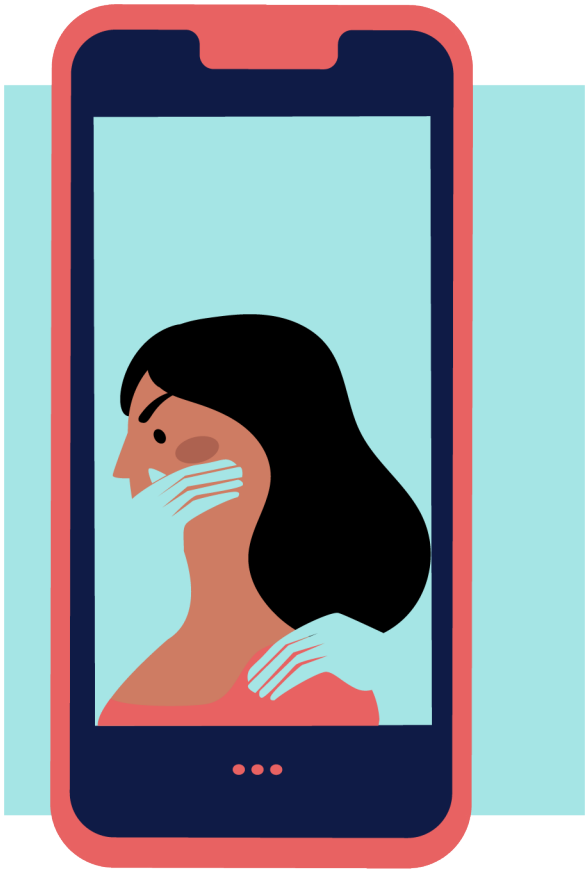
CONTRA LAS MUJERES Y LAS NIÑAS FACILITADA POR LAS NUEVAS TECNOLOGÍAS

Es importante no perder de vista que la violencia de género en línea contra las mujeres es una expresión que abarca una amplia variedad de prácticas y comportamientos dañinos u ofensivos y contextos *online-offline* que se transforman a la par de los avances tecnológicos.

Aquello que entendemos como violencia en línea contra las mujeres son, de hecho, prácticas y conductas muy diversas que pueden constituir ciberdelitos o actos ilícitos que conllevan responsabilidad administrativa, civil o penal de acuerdo con el derecho de cada país (IGF, 2015; REVM-ONU, 2018; APC, 2017).

Hasta la fecha persiste una gran disparidad en cuanto a la terminología utilizada para hacer referencia a los diversos tipos de violencia en línea contra las mujeres y sus manifestaciones, con constantes variaciones entre las expresiones usadas por los Estados, los organismos internacionales, las organizaciones no gubernamentales y el sector académico (Van Der Wilk, 2018). Desafortunadamente, eso ha sembrado la confusión en torno a la clasificación de estas conductas y, en muchos casos, ha dado lugar a referencias imprecisas en la legislación nacional.

En un esfuerzo por clarificar este escenario, **a continuación se presenta una guía descriptiva de las conductas y ataques en línea o facilitados por las TIC que podrían calificarse como formas específicas de violencia contra las mujeres y niñas basada en su género,** con miras a facilitar la identificación de experiencias personales y, a partir de ello, saber qué medidas se pueden tomar para fortalecer la seguridad digital de las víctimas (véase tercera parte de esta guía).



Este catálogo se conformó sobre la base de una revisión bibliográfica y no debe considerase como algo fijo o estático, puesto que la violencia digital está en constante transformación paralelamente a la tecnología y surgen otras manifestaciones de violencia a medida que aparecen nuevas herramientas tecnológicas (UNBC, 2015).

Asimismo, como se observará en este apartado, es importante tener en cuenta que puede haber casos en que dos o más formas de violencia digital se ejerzan de forma simultánea, sean interdependientes (por ejemplo, amenazas en línea seguidas de la distribución no consensuada de imágenes íntimas) o estén acompañadas de otras formas de violencia fuera de internet (como sucede a menudo en casos de violencia doméstica).

En todo caso, debe tenerse presente que estos ciberataques y actos en línea serán considerados como violencia de género al dirigirse contra una mujer por el mero hecho de ser mujer (es decir, por su identidad de género) o porque la afectan en forma desproporcionada.

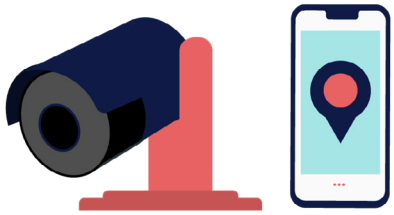
Tipos de violencia de género contra mujeres y niñas facilitada por las nuevas tecnologías:

01 Creación, difusión, distribución o intercambio digital de fotografías, videos o audioclips de naturaleza sexual o íntima sin consentimiento.

Acceso, uso, manipulación, intercambio o distribución no autorizados de datos personales. 02

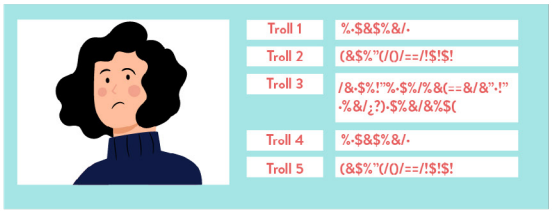
03 Suplantación y robo de identidad.

Actos que dañan la reputación o la credibilidad de una persona. 04

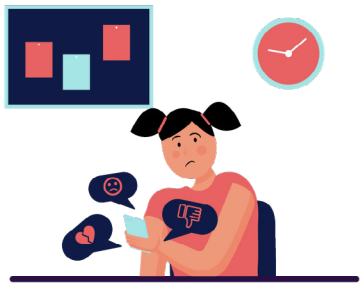


05 Actos que implican la vigilancia y el monitoreo de una persona.

Ciberhostigamiento. 06



07 Ciberacoso.



Ciberintimidación. 08

09 Amenazas directas de daño.

Violencia física facilitada por las tecnologías. 10

11 Abuso, explotación de mujeres y niñas a través de las tecnologías.

Ataques a grupos, organizaciones o comunidades de mujeres. 12

A

Creación, difusión, distribución o intercambio digital de fotografías, videos o audioclips de naturaleza sexual o íntima sin consentimiento

Las mujeres son las principales víctimas de esta forma de violencia digital, que las afecta de manera desproporcionada en todo el mundo. En varios estudios se ha comprobado que 90% de las personas afectadas por la distribución digital de imágenes íntimas sin consentimiento son mujeres (REVM-ONU, 2018; *Cyber Civil Rights Initiative*).

Consiste en crear, compartir o difundir en línea, **sin consentimiento**, material, imágenes o videos íntimos o sexualmente explícitos obtenidos con o sin el consentimiento de una persona, con el propósito de avergonzarla, estigmatizarla o perjudicarla (REVM-ONU, 2018, párr. 41).

Esta forma de violencia puede ocurrir en una gran variedad de contextos y relaciones interpersonales: en una relación íntima y de confianza en la cual estas imágenes son enviadas de forma voluntaria por una persona a su pareja o expareja sentimental (quizás por *sexting*), como parte de esquemas de ciberhostigamiento o ciberacoso por amistades, conocidos o desconocidos, o cuando el material se obtiene mediante *hackeo*[8] o acceso físico a dispositivos.

Abarca también los siguientes actos:

01 Grabar y distribuir imágenes de abuso sexual.

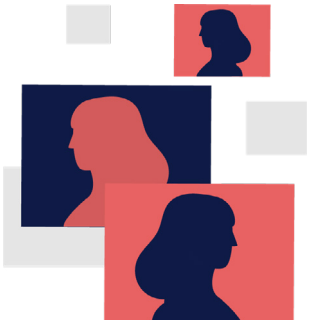
02 Tomar, sin consentimiento, fotografías o videos de partes íntimas del cuerpo de las mujeres en espacios públicos y compartirlos en línea (por ejemplo, fotografías tomadas por debajo de la falda o por arriba de la blusa, actos que se denominan *upskirting, downblousing o creepshots*).

03 **Crear imágenes sexualizadas, editadas con fotomontaje, o videos *deepfake*,** en cuyo caso las imágenes o los videos de las mujeres pueden ser tomados de sitios en línea o cuentas de redes sociales y superpuestos en el cuerpo de otras personas para simular escenas sexuales o contenido pornográfico con el objetivo de dañar la reputación de la víctima.

[8] El *hackeo* es el uso de técnicas y procedimientos por un hacker para introducirse sin autorización en sistemas informáticos ajenos con el fin de manipularlos o de obtener información o por diversión. El *cracking* es una práctica relacionada con el hackeo, pero implica entrar en sistemas ajenos con fines delictivos para violar la intimidad de la persona afectada o la confidencialidad de la información o dañar la información o los soportes físicos.

¿Qué es un *deepfake* (video ultra falso)?

Desde 2017 existen programas de *software* que utilizan técnicas de aprendizaje automático para intercambiar la cara de una persona con la de otra (Knight, 2019). Estos programas se están usando para crear videos pornográficos falsos y publicarlos en línea (Farokhmanesh, 2018). Con estos videos se ha atacado en particular a mujeres que participan en la vida política; sin embargo, se prevé que su uso se extenderá puesto que esta tecnología se ha vuelto más accesible para usuarios que no son expertos (*Deeptrace*, 2019). Además, dado que los videos *deepfakes* utilizan técnicas de aprendizaje automático, a la larga podría ser difícil distinguir entre un video falso y uno real sin la ayuda de herramientas forenses (Maras y Alexandrou, 2018).



La producción de fotografías o videos íntimos sin consentimiento **puede estar acompañada de extorsión o amenazas de distribuirlos** o efectuarse sin el conocimiento de las víctimas en grupos cerrados de redes sociales en los cuales varios hombres difunden imágenes de mujeres desnudas sin su consentimiento para gratificación sexual de los otros miembros o como parte de esquemas de enriquecimiento en los cuales los agresores compilan y venden enlaces con archivos o "paquetes" de imágenes sexuales de mujeres obtenidas por diversas vías sin su consentimiento (archivos que, en países como México y Chile, se han denominado *packs*)[9].

También **es muy común filtrar datos personales de las mujeres que aparecen en esas imágenes o videos,** muchas de las cuales se ven obligadas a abandonar la escuela, el trabajo, el hogar y su comunidad para evitar la humillación constante (Henry, Powell y Flynn, 2017).

Para recordar...

Esta forma de violencia en línea se ha denominado comúnmente "pornovenganza". Sin embargo, no es un término correcto, y su uso es problemático puesto que no refleja la diversidad de motivaciones de los perpetradores, que se extienden más allá de la venganza y van desde una reafirmación de su masculinidad hasta la extorsión económica o la gratificación sexual. Este término también minimiza el daño que se causa a las víctimas, oculta el componente no consensual de la conducta y pone énfasis en la imagen en lugar del comportamiento abusivo de los perpetradores (Powell, Henry y Flynn, 2018).

¿Qué es el *sexting* o sexteo?

El *sexting* o sexteo o es una práctica que implica la generación e intercambio de material sexualmente explícito (UNDOC, 2019; *Interagency Working Group*, 2016). Puede incluir la creación y envío de imágenes de forma consensuada o la creación consensuada de imágenes que se distribuyen sin consentimiento (Salter, Crofts y Lee, 2013, p. 302).

En varios estudios se ha comprobado que es una práctica común entre jóvenes de ambos sexos, quienes están utilizando las tecnologías como una herramienta de expresión sexual. Se ha constatado, sin embargo, que el *sexting* se presenta en contextos en los cuales las jóvenes y las niñas están sometidas a una mayor presión social que los jóvenes para compartir imágenes sexuales y degradantes de su cuerpo, mientras que los jóvenes y los niños se ven presionados para solicitar imágenes, recibirlas y compartirlas con sus amigos a fin de reafirmar su heterosexualidad (Walker, Sanci y Temple, 2013).

[9] Monserrat Peralta (2019). "El oscuro negocio de los packs". *El Universal.* Disponible en: https://www.eluniversal.com.mx/nacion/el-oscuro-negocio-de-los-packs-fotos-intimas-desde-un-peso-en-la-red

Bajo la lupa:
Algunos aspectos importantes del sexting y la distribución de imágenes y videos íntimos sin consentimiento:

01

Aunque exista consentimiento para intercambiar fotos íntimas con alguien o para grabar actos sexuales (incluso en presencia de otras personas), **este consentimiento no implica un permiso para almacenar, publicar, reproducir o difundir estos contenidos.** Haber consentido a la grabación no significa que se haya otorgado consentimiento para otra etapa en el proceso. Quien lo haga estará violando la intimidad de la persona que participó en la práctica de *sexting*. Esto es una forma grave de violencia de género, una violación de los derechos humanos, un acto ilícito, y ya está tipificado como delito en muchos países.

02

No se debe estigmatizar la práctica del *sexting*. Todas y todos tenemos derecho a usar la tecnología para expresar nuestra sexualidad. No obstante, al hacerlo es muy importante tener presente que hay riesgos y que, por consiguiente, es necesario **considerar la seguridad digital.**

03

Los Estados tienen la obligación de adoptar medidas apropiadas para prevenir, investigar, sancionar y reparar los daños causados por esta forma de violencia. Asimismo, las plataformas de internet están obligadas a evitar la difusión de imágenes y videos íntimos sin consentimiento, a retirar ese contenido y a reducir o mitigar los riesgos.

En el sitio Acoso.online se puede encontrar información sobre esta forma de violencia digital, así como consejos para denunciar un caso ante plataformas de internet, además de detalles sobre las distintas leyes en países de América Latina en las que puede basarse una denuncia. El sitio de la organización *Without my Consent* también tiene una gran variedad de recursos para apoyar a las sobrevivientes de esta forma de violencia[10]. Además, en la página 51 de esta guía se pueden encontrar algunas recomendaciones y consejos adicionales.

Se destaca que la provisión de estos recursos no representa un respaldo por parte de la OEA o de sus Estados Miembros al contenido o a las organizaciones aquí nombradas. Estos recursos se presentan a modo de ejemplo de aquellas organizaciones, guías, herramientas, etcétera, que están disponibles en la región para que las personas lectoras puedan ampliar la información relacionada con la temática de esta publicación.

[10] Acoso.online, *Pornografía no consentida. Cinco claves para denunciar y resistir su publicación.* Disponible en: https://acoso.online/ar; *Without my Consent. Tools to fight online harassment, Resources.* Disponible en: https://withoutmyconsent.org/resources/

B

Acceso, uso, control, manipulación, intercambio o publicación no autorizada de información privada y datos personales

Según Amnistía Internacional, una cuarta parte de las mujeres usuarias de internet han sido víctimas de *doxxing* al menos una vez en su vida (AI, 201).

Esta forma de violencia se manifiesta en forma de **ataques a cuentas en línea o dispositivos** de una persona (teléfonos móviles, computadoras, tabletas, etc.) para obtener, manipular y/o publicar información de manera no autorizada mediante el robo de contraseñas, instalación de programas espías, robo de equipo o registradores de teclas[11] (APC, 2017). Puede involucrar también el acceso no autorizado y control total de cuentas o dispositivos de una persona.

Doxing o *doxxing*:

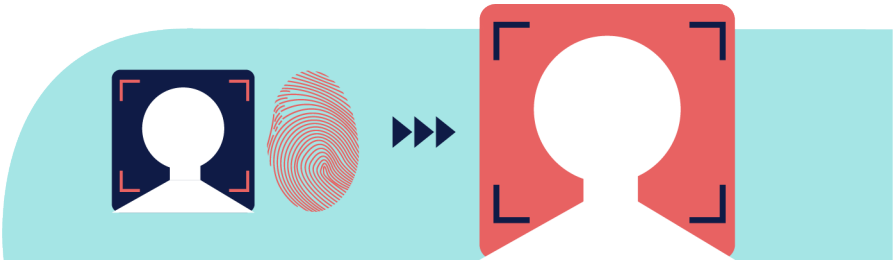
El término proviene de la frase en inglés *dropping docs* y consiste en **la extracción y la publicación no autorizadas de información personal** —como el nombre completo, la dirección, números de teléfono, correos electrónicos, el nombre del cónyuge, familiares e hijos, detalles financieros o laborales— como una forma de intimidación o con la intención de localizar a la persona en "el mundo real" para acosarla (APC, 2017; *Women's Media Center*, 2019). También se ha observado que la información personal puede ser publicada en sitios pornográficos junto con el anuncio de que la víctima está ofreciendo servicios sexuales.

[11] El registrador de teclas o *keylogger* es un programa malicioso que se instala entre el teclado y el sistema operativo para interceptar y registrar información de cada tecla pulsada en el dispositivo sin que la persona usuaria lo sepa.

c

Suplantación y robo de identidad

Una investigación realizada por la Universidad Nacional de Australia reveló que las mujeres tienen 50% más de probabilidades que los hombres de ser víctimas de robo de identidad[12].



Es una actividad malintencionada que consiste en **hacerse pasar por otra persona en línea usando sus datos personales con el fin de amenazarla o intimidarla** (*Women's Media Center*, 2019). Esto puede hacerse mediante la creación de perfiles o cuentas falsas en redes sociales o la usurpación de cuentas de correo o números de teléfono que puedan ser utilizados para contactar amistades, familiares, colegas o conocidos de la víctima con el propósito de entablar comunicación y tener acceso a información sobre ella (APC, 2017; Barrera, 2017).

El caso del ciberatacante de toda una familia

En un conocido caso en Chile, un agresor cibernético extranjero acosó durante 13 años a una familia completa y su círculo de amistades (al menos 50 personas), robando información personal y suplantando su identidad, incluido el robo de contraseñas, correos electrónicos y perfiles de redes sociales, así como fotos personales para enviar mensajes obscenos y hacer publicaciones a gran escala en páginas pornográficas. El agresor, que se sospecha que era la expareja sentimental de una de las integrantes de la familia, realizó numerosos actos de ciberviolencia contra toda persona relacionada con la víctima original y su familia o que tuviera contacto con ella (Paz Peña, 2017).

En casos de violencia doméstica es frecuente la suplantación y el robo de identidad de las víctimas a través de distintos mecanismos, como la utilización de sus datos personales para el uso ilícito de sus tarjetas de crédito o el control de los bienes, para controlar las comunicaciones que entablan con otras personas, o hacerse pasar por familiares o amistades en redes sociales para vigilarlas a través de esos perfiles.

[12] Australian Communications Consumer Action Network, "Identity Theft and Gender". Disponible en: https://accan.org.au/files/Grants/ANU%20ID%20theft/ANU%20ID%20theft%20infographic_Gender.pdf

D

Actos que dañan la reputación o la credibilidad de una persona

En una investigación mundial de la UNESCO, 41% de las encuestadas señaló haber sido blanco de ataques que parecían estar relacionados con campañas de desinformación dirigidas específicamete a desacreditar mujeres periodistas.

Esta forma de violencia afecta a las mujeres en general. Por ejemplo, de acuerdo con el estudio *Conocer para resistir. Violencia de género en línea en Perú* [13], 15% de las víctimas entrevistadas señalaron haber sido afectadas por la difusión de información falsa, manipulada o fuera de contexto.

Esta forma de violencia consiste en **crear y compartir información personal falsa con la intención de dañar la reputación de una persona.** Por ejemplo, crear perfiles falsos en redes sociales o cuentas en línea; hacer fotomontajes o imágenes manipuladas de contenido sexual a partir de fotografías obtenidas de redes sociales; publicar avisos en sitios de citas o pornográficos con fotos íntimas; difundir comentarios o publicaciones ofensivos o falsos o memes en foros de discusión, redes sociales o páginas de internet (incluidos los actos de vandalismo en *Wikipedia*) y realizar actos de calumnia y manipulación (APC, 2017; Barrera, 2017).

¿?

¿Qué es el *slutshaming*?

Es una forma de violencia que consiste en señalar públicamente a una mujer por su supuesta actividad sexual con el fin de avergonzarla, dañar su reputación y regular su sexualidad. Puede implicar el uso de fotografías y/o videos y lenguaje denigrante.

Caso Camila Zuluaga

Diversas organizaciones de la sociedad civil han documentado a lo largo de la región un aumento en la comisión de actos en línea que buscan dañar la reputación y credibilidad de mujeres periodistas, políticas y defensoras de derechos humanos (Peña, 2017; Luchadoras, 2017; Cuellar y Chaher, 2020). En un caso en Colombia, la periodista Camila Zuluaga fue atacada en septiembre de 2019 de forma coordinada y masiva luego de que el portal *Los Irreverentes* publicó, sin presentar prueba alguna, que había recibido 35 millones de pesos de una persona implicada en un escándalo de corrupción. Los ataques se concentraron en las etiquetas #CamilaEstásPillada y #CamilitaEstásPillada, que alcanzaron hasta 10 mil menciones en un día. Investigaciones en el tema encontraron evidencias de automatización en estos ataques coordinados y la operación de un grupo de WhatsApp en el cual se daban las instrucciones para realizar los ataques a fin de desprestigiar su trabajo periodístico (Cuellar y Chaher, 2020).

[13] UNESCO y el Centro Internacional para Periodistas (ICFJ) (2021). Violencia en línea: La nueva línea de combate para las mujeres periodistas - #JournalistsToo. Disponible en: https://unesdoc.unesco.org/ark:/48223/pf0000375136_spa; Carlos Guerrero y Miguel Morachimo (2018). Conocer para resistir. Violencia de Género en Línea en Perú. Disponible en: https://hiperderecho.org/tecnoresistencias/wp-content/uploads/2019/01/violencia_genero_linea_peru_2018.pdf

Actos que implican la vigilancia y el monitoreo de una persona

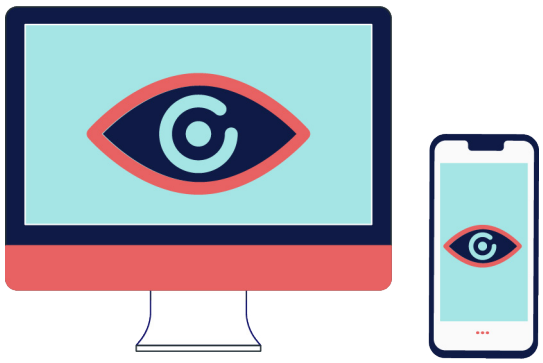
Se ha documentado que, por lo menos en 29% de los casos de violencia doméstica o íntima, la pareja o expareja ha usado algún tipo de programa espía o equipo de geolocalización instalado en las computadoras o los celulares de las mujeres afectadas (*Women's Aid*, 2014).

El monitoreo y la vigilancia constantes de las **actividades de una persona en línea y fuera de internet** o de su ubicación constituyen formas de violencia que pueden realizarse con la intervención de diferentes tecnologías (APC, 2017).

- Se pueden realizar con un *spyware* instalado en el celular de la víctima para monitorearla clandestinamente o robar su información.
- También se efectúan con dispositivos de geolocalización ubicados en automóviles o en bolsas de mano, juguetes, cámaras de vigilancia, asistentes virtuales o dispositivos inteligentes conectados.

¿Qué es el *spyware*?

Es un tipo de *software* malicioso que se instala en los dispositivos de una persona para registrar todo lo que hace, incluidos los mensajes de texto, los correos electrónicos, las fotografías o hasta todas las teclas pulsadas. Con ciertos tipos de *software* malicioso, los agresores pueden encender de forma remota la cámara o el micrófono del teléfono móvil, rastrear la ubicación de la víctima, monitorear el uso de aplicaciones o interceptar llamadas.



F

Ciberhostigamiento o ciberacecho

Varios estudios sobre el tema han demostrado que el ciberhostigamiento y el ciberacoso son ciberdelitos con una importante connotación de género y que las mujeres y las niñas tienen una mayor probabilidad de ser víctimas de estas formas de violencia (Reyns, Henson y Fisher, 2011).

Hasta la fecha no hay una definición única del ciberhostigamiento, ya que abarca una gran variedad de comportamientos digitales abusivos. En términos generales puede definirse como una actividad intencional y reiterada realizada mediante computadoras, teléfonos celulares y otros dispositivos electrónicos, que puede constituir o no actos inofensivos por separado, pero que, en conjunto, constituye un patrón de conductas amenazantes que socavan la sensación de seguridad de una persona y le provocan miedo, angustia o alarma (EIGE, 2017: 4; PRC, 2018; Maras, 2016). Esta actividad puede estar dirigida también contra familiares, amistades o la pareja sentimental de la víctima.

A diferencia del ciberacoso, el ciberhostigamiento implica un patrón y la comisión de más de un incidente a lo largo de un tiempo usando las TIC, con el objetivo reiterado de hostigar, acechar, molestar, atacar, humillar, amenazar, asustar u ofender a una persona o abusar verbalmente de ella (UNODC, 2015). Puede consistir en correos electrónicos, llamadas, mensajes de texto, chat en línea o el envío constante de comentarios obscenos, vulgares, difamatorios o amenazantes por internet. Algunas de las conductas que puede abarcar son:

Espiar, obsesionarse o compilar información en línea sobre alguien y entablar comunicación con la persona sin su consentimiento; enviar constantemente solicitudes de amistad en redes sociales; unirse a todos los grupos en línea de los que esta forma parte; dar seguimiento a las notas publicadas por la víctima en redes sociales por medio de conocidos que tengan en común, colegas, amistades o familiares, o ver constantemente su perfil para que ella lo note (UNODC, 2019).

Llamar o enviar correos, mensajes de texto o de voz de forma repetitiva, incluso mensajes amenazantes o que busquen mantener el control sobre la víctima.

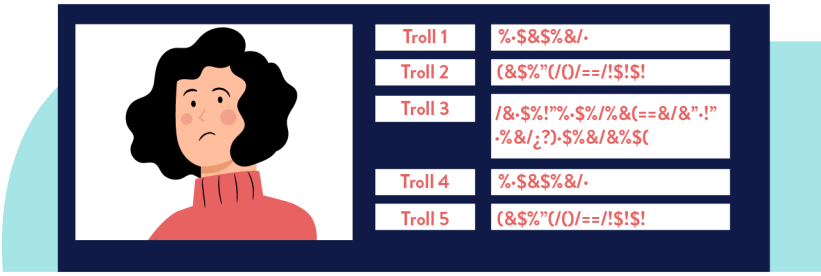
Formular proposiciones sexuales indeseadas y reiteradas, enviar fotos sexuales no solicitadas (fotos de los genitales masculinos de los agresores) o monitorear y vigilar constantemente la ubicación de una persona o sus actividades y comunicaciones diarias (Henry y Powell, 2016).

Publicar constantemente información falsa, maliciosa u ofensiva sobre una persona en sus páginas, blogs o redes sociales.

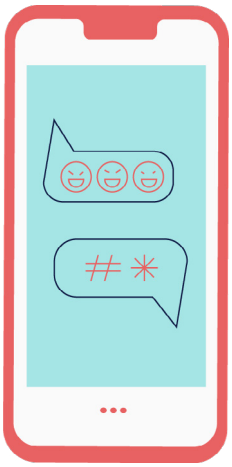
Los perpetradores de ciberhostigamiento pueden ser parejas íntimas o sexuales, exparejas, conocidos, amistades, familiares o extraños. También es importante destacar que **esta táctica es particularmente frecuente en contextos de violencia doméstica o de pareja.**

Ciberacoso

En un estudio publicado en 2018 por Amnistía Internacional se señaló que 23% de las mujeres encuestadas habían experimentado por lo menos una vez algún tipo de abuso u hostigamiento en redes sociales (AI, 2018).



El ciberacoso implica el **uso intencional de las TIC para humillar, molestar, atacar, amenazar, alarmar, ofender o insultar a una persona** (Maras, 2016). A diferencia del ciberhostigamiento, en el que hay un patrón de comportamientos amenazantes, en el caso del ciberacoso basta con un solo incidente, aunque puede implicar también más de uno (UNODC, 2019).



El ciberacoso **puede adoptar numerosas manifestaciones y estar asociado a otras formas de violencia en línea.** Por ejemplo, puede incluir el envío de mensajes no deseados e intimidantes por correo electrónico, texto o redes sociales; insinuaciones inapropiadas u ofensivas en redes sociales o salas de chat; violencia verbal y amenazas en línea de violencia física o muerte; discurso de odio; el robo o la publicación de información personal, imágenes y videos, y la difusión de información falsa o rumores para dañar la reputación de una persona (EIGE, 2017; APC, 2017, UNODC, 2019).

¿Qué es el discurso de odio?

Es el uso de un lenguaje que denigra, insulta, amenaza o ataca a una persona a causa de su identidad y otras características, como su orientación sexual o discapacidad.

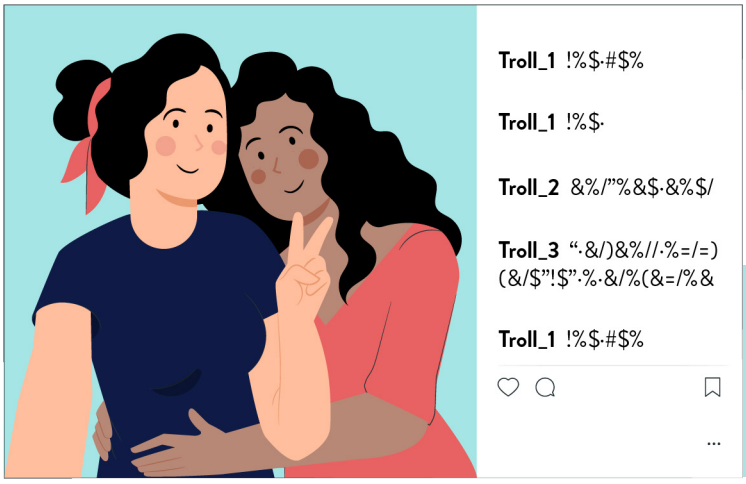
El ciberacoso puede abarcar también la revelación de información personal de la víctima (*doxxing*) con invitaciones a su violación sexual, lo cual ha propiciado situaciones de revictimización en las cuales los acosadores y agresores van al domicilio de la mujer bajo ataque.

El ciberacoso, que afecta de forma desproporcionada a las mujeres en todo el mundo, tiene connotaciones sexuales (Li, 2006; Henry y Powell, 2017, p. 212). Puede implicar amenazas de violación, femicidio, violencia física sexualizada o incitación a la violencia física y sexual dirigida contra la víctima o sus familiares, y ataques verbales sexistas u ofensivos asociados a la condición de género o a la apariencia física de las mujeres. Incluye el envío indeseado de materiales sexualmente explícitos, contenido que deshumaniza a las mujeres y las presenta como objetos sexuales, *slutshaming* o comentarios misóginos, explícitamente sexuales y abusivos (Jane, 2016).

¿Sabías que...?

Varios estudios revelan que las mujeres tienen más del doble de probabilidades que los hombres de ser blanco de ciberacoso sexual (Reid, 2016).

Una forma común de ciberacoso sexual es el *cyberflashing* o envío de fotos obscenas a una mujer sin su consentimiento (por ejemplo, fotografías de los genitales del acosador) con el objetivo de molestarla, intimidarla o incomodarla.

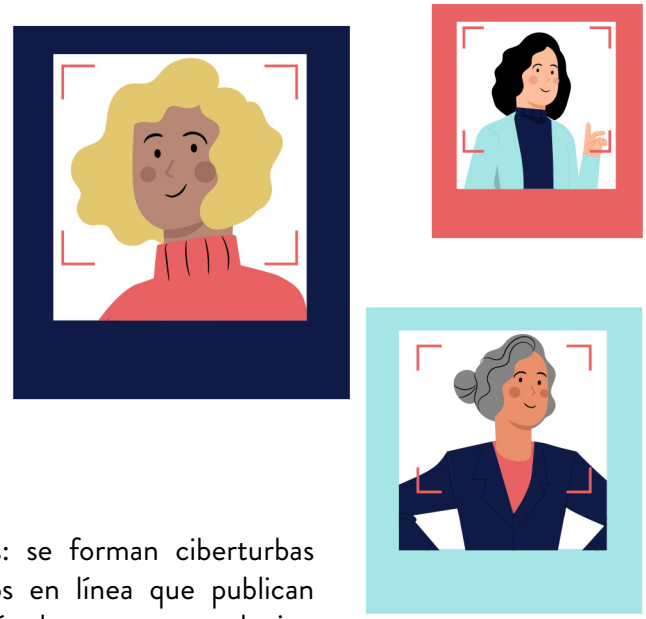


Los perpetradores de ciberacoso pueden ser *trolls*, que publican comentarios extremadamente ofensivos y virulentos para provocar una reacción emocional y una respuesta de otras personas usuarias de internet. Este comportamiento se denomina *troleo* (Maras, 2016).

El *troleo* de género es la publicación de mensajes, imágenes o videos, así como la creación de *hashtags*, con el propósito de molestar a mujeres y niñas o incitar a la violencia contra ellas (REVM-ONU, 2018; Mantilla, 2013)

El ciberacoso también puede ser grupal (a lo que se ha llamado *raiding*), cuando dos o más personas se organizan y se coordinan para acosar en línea de forma repetida a una persona, muchas veces de manera sostenida a lo largo del tiempo y con una estrategia. Estos grupos pueden estar formados por miembros de comunidades, foros o alianzas digitales, donde se han encontrado ciertos tipos de masculinidades particularmente violentas (Jane, 2017). El ciberacoso puede realizarse también a través de *bots* y/o cuentas falsas (llamadas marionetas o *sockpuppets*) que buscan pasar como usuarios reales para difundir información sesgada, desinformar o atacar.

Están proliferando en América Latina los ataques de grupos coordinados por medio de redes de troles y hackers, como la "Legión Holk" (originada en Colombia y Perú) o la "Secta 100tifika", que realizan ataques y acoso en masa con el fin de generar confrontación y polémica, generar tendencias y fomentar la discriminación, el racismo y la misoginia. Estos grupos suelen atacar a mujeres que son activas en redes sociales, que tienen un perfil público o que son feministas. Es común la difusión de fotomontajes sexualizados, la suplantación de su identidad en redes sociales con fines difamatorios y la circulación de contenidos degradantes (Peña, 2017; Barrera, 2017).



Algunos de estos ataques se han vuelto desproporcionados: se forman ciberturbas (denominadas *cybermobs*) integradas por grupos organizados en línea que publican contenido ofensivo o destructivo de forma masiva con la intención de avergonzar a alguien o de lograr el retiro de su perfil de redes sociales (Citron, 2014).

Caso Ana Gabriela Guevara

Un caso emblemático de ataques coordinados en México fue el de la ex deportista y senadora Ana Gabriela Guevara, quien, en diciembre de 2016, después de haber hecho públicas en redes sociales las agresiones físicas que sufrió en la vía pública, fue atacada por grupos organizados de *trolls y hackers* con cuentas falsas que hicieron virales *hashtags* con referencias a la violencia de género. Se utilizaron *hashtags* tales como #MujerGolpeadaEsMujerFeliz o #GolpearMujerEsFelicidad, los cuales se convirtieron en t*rending topics* en diversos países hispanohablantes (Peña Ochoa, 2017; Barrera, 2017).

Ciberbullying

Según una investigación a nivel mundial realizada por IPSOS[14] en 2018, 1 de cada 5 progenitores señaló que su hija/o había sido víctima de *ciberbullying*. También se identificó que Perú, Argentina y México eran los países con los niveles más altos de *ciberbullying* en redes sociales.

El *ciberbullying* o ciberintimidación es el uso de tecnologías por menores de edad para humillar, molestar, alarmar, insultar o atacar a otra/o menor de edad o difundir información falsa o rumores sobre la víctima, así como para amenazarla, aislarla, excluirla o marginarla (Maras, 2016; Hinduja y Patchin, 2014; UNODC, 2015).

Puede realizarse a través de mensajes de texto, correos electrónicos, encuestas virtuales, blogs, publicaciones de redes sociales, videojuegos en línea o sitios de realidad virtual, y puede producir daños muy graves a la salud emocional y física de las personas bajo ataque, quienes pueden incluso autolesionarse o suicidarse.

En la mayoría de los países se considera que, **en los casos de *ciberbullying*, los niños y las niñas son responsables y víctimas de esta forma de violencia** (Duggan et al., 2015). En otros, como Australia y Nueva Zelandia, el *ciberbullying* puede involucrar a personas adultas.

¿Sabías que...?

Hay diversas opiniones sobre si el género de las personas es un factor determinante del *ciberbullying* (Navarro y Jasinski, 2013; Smith, 2012; Fanti, Demetriou y Hawa, 2012; Livingstone et al., 2011; Calvete et al., 2010). A reserva de ello, es claro es que los daños y las consecuencias que sufren las niñas y los niños son diferentes en función de los estereotipos de género que enfrentan: es común que las niñas víctimas de *ciberbullying* sean atacadas con comentarios ofensivos y violentos sobre su cuerpo o su sexualidad.

[14] Ipsos Public Affairs (2018). *Cyberbullying. A Global Advisory Survey.* Disponible en: https://www.ipsos.com/sites/default/files/ct/news/documents/2018-06/cyberbullying_june2018.pdf

1

Amenazas directas de daño o violencia

En 2019, Amnistía Internacional publicó la investigación *Corazones Verdes: Violencia online contra las mujeres durante el debate por la legislación del aborto en Argentina*[15], en la cual identificó que 1 de cada 3 mujeres encuestadas había sufrido violencia en redes sociales, de las cuales 26% recibió amenazas directas y/o indirectas de violencia psicológica o sexual.

Este tipo de violencia consiste en el envío o la publicación de comunicaciones o contenido (mensajes orales o escritos, imágenes, videos) por medio de tecnologías para expresar la **intención de cometer un daño** físico o violencia sexual (APC, 2017; Barrera, 2017).

Incluye la extorsión digital, la cual ocurre cuando una persona ejerce presión sobre otra para forzarla a actuar de un cierto modo con amenazas, intimidación o agresiones, con la finalidad de doblegar su voluntad o controlarla emocionalmente. Puede tomar la forma de amenazas de publicar en línea o enviar a conocidos de la víctima información privada, sexual o íntima como chantaje sexual.

¿Qué es la sextorsión?

La sextorsión consiste en amenazar a una persona con difundir imágenes o videos íntimos con la finalidad de obtener más material sobre actos sexuales explícitos, mantener relaciones sexuales o sonsacar dinero (REVM-ONU, 2018, párr. 32). Esta forma de violencia afecta desproporcionadamente a mujeres y, con pocas excepciones, es perpetrada por lo general por personas que se identifican como hombres (Kelley, 2019).

Esta forma de violencia ha tenido un crecimiento exponencial durante los últimos años y puede llevarse a cabo de múltiples formas: desde *hackers* que envían correos en los que exigen dinero para no publicar imágenes y videos íntimos supuestamente tomados de forma remota activando la cámara de un dispositivo hasta parejas o exparejas íntimas que hacen sextorsión para su propia gratificación sexual. En un informe de 2018 del Centro de Quejas sobre Delitos Cibernéticos del FBI, se señaló que se había producido un incremento de 242% de los correos electrónicos con amenazas de extorsión, que en su mayoría son sextorsivos (FBI-ICC, 2018).

[15] Amnistía Internacional (2019). *Corazones Verdes. Violencia online contra las mujeres durante el debate por la legalización del aborto en Argentina.* Disponible en: https://amnistia.org.ar/corazonesverdes/files/2019/11/corazones_verdes_violencia_online.pdf

Caso #GamerGate

En 2014 tuvo lugar una de las primeras campañas de ataques masivos en línea denominada *#GamerGate*[16] dirigida en contra de varias mujeres de la industria de los videojuegos, incluidas las desarrolladoras Zoe Quinn, Brianna Wu y la comunicadora Anita Sarkeesian, luego de que se pronunciaran en torno al sexismo y la desigualdad de género en los videojuegos. Los partidarios del *#GamerGate* manifestaron su oposición a la influencia del feminismo en la cultura de los videojuegos, organizándose en plataformas en línea tales como *4Chan, Twitter* y *Reddit* para coordinar ataques a gran escala que incluyeron actos de ciberacoso, *doxxing* y amenazas de violación y de muerte. Estas tres mujeres denunciaron ataques de *doxxing* con amenazas que escalaron a tal magnitud que tuvieron que huir de sus casas. En particular, los ataques en contra de Anita Sarkeesian alcanzaron proporciones altamente agresivas que incluyeron amenazas de bomba cuando se le nominó para recibir un premio en San Francisco y amenazas terroristas cuando se anunció que participaría en una conferencia en la Universidad de Utah.

Violencia física facilitada por las tecnologías

En la investigación de la UNESCO y ICFJ titulada *Violencia en línea: La nueva línea de combate para las mujeres periodistas - #JournalistsToo*[17] se documentó que 20% de las mujeres encuestadas habían sido atacadas *offline* en conexión con la violencia que experimentaron en línea.

Esta forma de violencia puede tener diversas manifestaciones, como ataques sexuales organizados o planificados por medio de las TIC o violencia sexual a partir de la publicación en línea de los datos personales de la víctima después de localizarla (*doxxing*).

También puede presentarse cuando un agresor entabla amistad en línea con una persona para conocerla y después abusar sexualmente de ella (como puede ocurrir con aplicaciones de citas) o cuando un agresor obliga a una persona a entablar relaciones sexuales bajo la amenaza de publicar información íntima o sexual (sextorsión) (Henry y Powell, 2018).

[16] Eliana Dockterman (2014). "What is #GamerGate and why are women being threatened about video games?" *Time*. Disponible en https://time.com/3510381/gamergate-faq/
[17] UNESCO y el Centro Internacional para Periodistas (ICFJ) (2021). *Violencia en línea: La nueva línea de combate para las mujeres periodistas - #JournalistsToo*. Disponible en: https://unesdoc.unesco.org/ark:/48223/pf0000375136_spa

Abuso, explotación y/o trata de mujeres y niñas por medio de las tecnologías

Algunas encuestas indican que las nuevas tecnologías facilitan la trata mundial de personas (cuyas víctimas son mujeres en 80% de los casos y en 95% de los casos de explotación sexual) con un nuevo *modus operandi* digital, en el cual se usa la internet para el reclutamiento, la venta, el anuncio y la explotación de mujeres y niñas (Van Der Wilk, 2018).

Esta forma de violencia en línea implica la intermediación de las tecnologías para el ejercicio de poder sobre una persona a partir de la explotación sexual de su imagen o de su cuerpo contra su voluntad (Barrera, 2017). Algunas de las conductas incluidas en esta forma de violencia son las siguientes:

- El uso de tecnologías para seleccionar y enganchar mujeres y niñas con fines de abuso sexual o trata, obligarlas a aceptar situaciones de trata y abuso sexual, ejercer poder y control sobre ellas o impedirles que se liberen del abuso, incluso con amenazas de revelar información privada (REVM-ONU, 2018, párr. 32).

- El *grooming* o ciberengaño pederasta, es decir, actos deliberados de un adulto para acercarse a una persona menor de edad (posiblemente cultivando una conexión sentimental) con el objetivo de establecer una relación y un control emocional que le permita cometer abusos sexuales, entablar relaciones virtuales, obtener pornografía infantil o traficar al o la menor (*Women's Media Center*, 2019).

- La publicación de imágenes sexuales sin el consentimiento de una persona para fines de comercialización y prostitución.

Ataques a grupos, organizaciones o comunidades de mujeres

Diversos estudios han documentado que entre quienes enfrentan un riesgo más alto de ser víctimas de violencia de género en línea se encuentran las defensoras de derechos humanos y de la igualdad de género, mujeres identificadas como feministas y mujeres activistas trabajando en el ámbito de la salud sexual y reproductiva (APC, 2017; Barrera, 2018; REVM-ONU, 2018)

Consisten en actos intencionales para censurar y dañar a organizaciones de mujeres, incluso con ataques a sus canales de expresión (Barrera, 2018), como tener acceso a ellos sin consentimiento y *hackear* páginas de internet, redes sociales o cuentas de correo para afectar el desarrollo de sus funciones, lograr que se dé de baja al perfil o a las redes sociales de la organización mediante el uso de normas comunitarias para denunciar contenido que la plataforma considera sensible, ataques de denegación de servicio (DDoS)[18], restricciones de uso de dominio o robo de dominio, y *blakouts* o apagones de internet durante una reunión o protesta (APC, 2017).

Abarcan la vigilancia y el monitoreo de las actividades de las integrantes de comunidades o grupos, amenazas directas de violencia contra ellas, el ciberacoso mediante contenido sexualmente explícito, la publicación de información confidencial (como direcciones de refugios para mujeres sobrevivientes de violencia) o el acoso reiterado a un grupo completo.

Casos de ataques a grupos feministas

En América Latina se han registrado múltiples ataques a sitios web, perfiles o cuentas de grupos feministas o defensoras de los derechos humanos de las mujeres con el fin de bloquear o poner fuera de línea sus contenidos de forma temporal o permanente. Se han denunciado casos como el de la colectiva feminista mexicana Las Hijas de la Violencia y la organización feminista colombiana Mujeres Insumisas, y constantes ataques coordinados contra activistas y grupos de mujeres feministas negras y transfeministas en Brasil (Lyons et al., 2016; Peña, 2017).

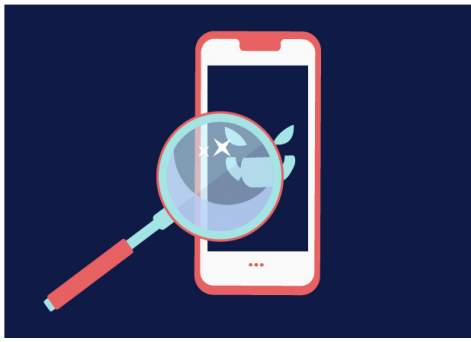
[18] Ataque en línea que consiste en movilizar personas para que envíen una gran cantidad de solicitudes al servidor de un sitio web a fin de saturarlo y que sea inaccesible.

Parte tres

PREVENCIÓN Y COMBATE DE LA VIOLENCIA EN LÍNEA CONTRA LAS MUJERES:

Una mirada desde las instituciones

Intervenciones para combatir la violencia en línea contra las mujeres y las niñas



Las medidas para prevenir, atender, investigar y sancionar los actos de violencia contra las mujeres facilitados por las nuevas tecnologías han recibido creciente atención a escala nacional e internacional. A medida que se ha ido percibiendo la extensión de este fenómeno y sus graves efectos en las mujeres y las niñas, varios sectores se han volcado a la búsqueda de medidas que permitan dar respuesta a las amenazas a la seguridad y la integridad de las mujeres que los rápidos cambios tecnológicos han traído aparejadas.

Algunos estudios iniciales y testimonios de víctimas y sobrevivientes han permitido encontrar elementos comunes que son sin duda una valiosa guía para el desarrollo de la capacidad institucional. Por ejemplo, se ha documentado la falta generalizada de información sobre las características de la violencia de género facilitada por las TIC y sobre las prácticas de seguridad digital que las mujeres pueden implementar para protegerse; se observa en diversos países una carencia de servicios de apoyo para las víctimas; persiste una gran necesidad de capacitación para autoridades de todos los niveles a fin de que puedan brindar una orientación adecuada; y se mantienen vigentes marcos jurídicos nacionales que dificultan el acceso a la justicia para las mujeres que sufren esta forma de violencia (Barrera, 2017; APC, 2017; Peña Ochoa, 2017; Van Der Wilk, 2018).

Asimismo, se ha comprobado que, con frecuencia, los órganos encargados de hacer cumplir la ley trivializan la violencia en línea contra las mujeres y culpan a las víctimas (más que a los agresores), lo cual se ha traducido en una cultura de silencio en que las sobrevivientes prefieren no informar a las autoridades sobre los actos de violencia ante el riesgo de ser ignoradas o revictimizadas durante el proceso (Abdul, 2017: p. 7; REVM-ONU, 2018, párr. 68).

La Relatora Especial sobre la Violencia contra la Mujer, de las Naciones Unidas, retomó en su informe sobre violencia digital publicado en 2018 diversas propuestas del Foro para la Gobernanza de Internet con respecto a medida estatales para responder a este fenómeno. Subrayó la obligación de los Estados de asegurar que tanto los agentes estatales como los no estatales se abstengan de incurrir en actos de violencia en línea contra las mujeres, así como de emplear la diligencia debida a fin de prevenir, investigar y sancionar estos actos (REVM-ONU, 2018, párr. 62). Entre algunas de las medidas señaladas por la Relatora Especial se encuentran las siguientes:

- Aplicar una perspectiva de género a todas las formas de violencia en línea.
- Tomar medidas para crear conciencia sobre el hecho de que la violencia en línea es una forma de violencia contra la mujer, una forma de discriminación y una violación de los derechos humanos.
- Recopilar y publicar datos desglosados por sexo sobre el acceso a internet, la prevalencia de la violencia en línea contra las mujeres y los daños que causa.
- Brindar servicios de asistencia rápidos, adecuados y accesibles para mujeres afectadas por esta forma de violencia, incluido el establecimiento de líneas telefónicas de asistencia y unidades especializadas de atención, además de difundir ampliamente información sobre dichos servicios a fin de que las mujeres conozcan su existencia.
- Proporcionar a las víctimas asistencia jurídica apropiada.
- Establecer mecanismos jurídicos que permitan investigar y sancionar diligentemente actos de violencia en línea contra las mujeres, además de ofrecer la posibilidad de solicitar órdenes de protección para las víctimas.
- Adoptar medidas efectivas para impedir la publicación de contenido perjudicial por motivos de género y para suprimirlo y evitar su distribución.
- Fomentar los conocimientos técnicos de las autoridades de procuración e impartición de justicia.
- Adoptar modelos de intervención, protocolos y códigos de conducta claros y especializados a fin de que los funcionarios puedan dar una respuesta oportuna a esta forma de violencia.
- Combatir la cultura de la impunidad de los perpetradores con la aplicación de sanciones adecuadas, necesarias y proporcionales al hecho delictivo.
- Otorgar reparaciones a las víctimas de violencia en línea de forma proporcional a la gravedad de los daños sufridos, una compensación financiera para sufragar los costos ocasionados por los daños materiales e inmateriales, medidas de restitución, rehabilitación y satisfacción y garantías de no repetición.
- Establecer un marco jurídico integral para combatir y prevenir la violencia contra la mujer facilitada por las TIC y para que los autores respondan ante la justicia por sus actos.
- Tomar medidas para eliminar toda desigualdad de género en el acceso a las tecnologías y promover la alfabetización digital.

Análogamente, las entrevistas de sobrevivientes de violencia doméstica facilitada por nuevas tecnologías y de personal especializado en la atención de la violencia contra las mujeres han proporcionado orientación sobre otras medidas que podrían adoptarse en este ámbito, entre ellas (Dragiewicz, 2019):

- Aumentar la educación y la sensibilización de las autoridades y el personal de primer contacto sobre las características y los efectos de esta violencia.
- Proporcionar capacitación adecuada a la policía sobre la obtención de pruebas de la violencia en línea contra mujeres y para brindar orientación a las sobrevivientes acerca de medidas de seguridad digital.
- Reconocer la brecha digital que afecta a muchas de las víctimas de violencia doméstica y responder a ella.
- Incorporar la capacitación sobre la violencia contra las mujeres facilitada por nuevas tecnologías en los currículos universitarios de las carreras de derecho, psicología y asistencia social.
- Facilitar la labor de especialistas en tecnología y seguridad para que proporcionen asesoramiento y asistencia a centros de atención y refugios para sobrevivientes de violencia (por ejemplo, con el análisis de posibles amenazas a la integridad digital de las mujeres que acuden a dichos centros).

Sin duda, ante la novedad del fenómeno, aún resta mucho por conocer sobre la realidad que enfrentan diariamente las víctimas de violencia digital por razones de género, y seguramente surgirán nuevos y renovados esquemas de intervención a medida que las mujeres exijan justicia y se tenga más conocimiento sobre los vínculos entre la violencia de género y las nuevas tecnologías.

Además, se requerirán las contribuciones y la participación no solo de autoridades nacionales, sino también de intermediarios de internet, representantes de víctimas, la sociedad civil, el sector académico y todas las partes interesadas que intervienen tanto en la gobernanza de internet como en las políticas nacionales y regionales de ciberseguridad y en las estrategias locales para erradicar la violencia contra las mujeres.

En este marco común de aprendizaje y trabajo colaborativo, tomando en cuenta el dinamismo de este tema y la necesidad de atenderlo adecuadamente, hay algunos **puntos importantes a considerar en las reflexiones que ya tienen lugar en torno a la violencia de género digital contra las mujeres,** así como en las que habrán de impulsarse en el futuro.

En primer lugar, la violencia en línea contra mujeres, como parte de la serie de formas múltiples, interrelacionadas y recurrentes de violencias por razones de género, **es un problema complejo, multicausal y multidimensional** con raíces sociales que van más allá de la mera intermediación de la tecnología y para el cual no existe una única solución, sino que **se requiere un enfoque multidisciplinario y la participación de diversos sectores.**

En segundo término, de acuerdo con las experiencias nacionales con la aplicación de modelos de intervención para combatir la violencia de género fuera de internet, será importante **adoptar una visión integral y holística, considerando el plano individual, familiar, comunitario y social, así como los efectos a escala global** que la violencia de género tiene en el acceso efectivo de las mujeres a las nuevas tecnologías y, con ello, en el desarrollo de una internet más justa e igualitaria que pueda beneficiar a todas las sociedades.

En tercer lugar, como se ha reafirmado a escala internacional, es fundamental tener presente que **se deben proteger los derechos humanos de las mujeres dentro y fuera de internet** y, en particular, reconocer el papel que desempeña en la revolución digital el derecho de las mujeres a tener acceso a internet en condiciones de igualdad y sin discriminación.

Por último, será crucial trabajar con una lógica que impulse **el empoderamiento digital de las mujeres y su seguridad en línea,** encarando este tema desde una visión que promueva su autonomía digital, reconozca su diversidad y cuestione los modelos que tratan a las mujeres como víctimas irremediables de agresiones en línea y ciberdelitos, negándoles su derecho fundamental a la seguridad y a la libertad de navegar en el mundo digital.

Sin duda, empoderar a niñas y mujeres de todas las edades para que rompan las barreras que las separan de las tecnologías y para que desarrollen un pensamiento estratégico sobre su seguridad digital es una estrategia toral que deberá encauzar esfuerzos colectivos en el futuro próximo. Esta ha sido, precisamente, la premisa bajo la cual se ha buscado estructurar esta guía y a partir de la cual se espera seguir impulsando más intervenciones en este ámbito.

B

¿Qué se está haciendo en los países de América Latina y el Caribe?

Durante los últimos años, diversos países de América Latina y el Caribe han iniciado un reconocimiento paulatino de la violencia en línea contra las mujeres y han actualizado su marco jurídico para hacerle frente, incluso con la promulgación de leyes específicas sobre el ciberhostigamiento, el ciberacoso, el *grooming* y el *ciberbullying*.

Particularmente, debido en gran medida a la atención prestada por los medios de comunicación y a las exigencias de la opinión pública, a lo largo del continente americano ha habido avances legislativos importantes en lo que se refiere a la distribución no consentida de imágenes íntimas o sexualmente explícitas (Neris et al., 2018).

En Paraguay, la Ley 19.580 promulgada en 2017 reconoció la violencia telemática, entendida como la difusión o publicación a través de las TIC de material audiovisual que afecta la dignidad o intimidad de las mujeres. Brasil promulgó en diciembre de 2018 la Ley 13.772/2018 para penalizar la grabación y almacenamiento no autorizado y la exposición de contenidos desnudos o sexuales. Según la ley, se consideran como casos de violencia doméstica aquellos en los que había una relación preexistente entre la víctima y el autor. Asimismo, cuenta con la Ley 13.718/18 que tipifica el crimen de divulgación de imágenes de violación sexual.

Mediante el Decreto Legislativo N.° 1410 de septiembre de 2018, Perú incorporó en el Código Penal los delitos de acoso, acoso sexual, chantaje sexual y difusión de imágenes, materiales audiovisuales o audios con contenido sexual a través del uso de las TIC. Por su parte, Chile adoptó en 2019 la Ley 21.153 mediante la cual se criminalizó la difusión no autorizada de material o imágenes íntimas registradas en lugares públicos sin consentimiento, y Nicaragua aprobó en octubre de 2020 la Ley de Ciberdelitos, la cual castiga las amenazas y el acoso a través de las nuevas tecnologías, así como la difusión de material sexual explícito.

En México son ya 28 las legislaturas locales en las cuales se han adoptado en total 35 reformas legislativas criminalizando la distribución no consentida de imágenes íntimas. A nivel federal, en abril de 2021 se aprobó una serie de reformas legislativas del Código Penal Federal y la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia las cuales reconocen la violencia digital y tipifican el delito de violación a la intimidad sexual de las personas a través de la distribución no consensuada de material íntimo sexual. A esta serie de reformas se le ha denominado "Ley Olimpia" a raíz de la labor realizada para el reconocimiento de esta forma de violencia digital por Olimpia Melo Cruz, quien en 2014 fuera víctima de la difusión no autorizada de un video de contenido sexual[19].

En Argentina, la Comisión de Reforma del nuevo Código Penal propuso la incorporación como delito informático de la difusión y grabación sin consentimiento de contenido sexual, conducta que a la fecha sólo está penada en el caso de menores de edad. El Código Contravencional de Buenos Aires ya incorpora como delito la difusión no consentida de imágenes o grabaciones íntimas y el hostigamiento digital.

Están en discusión otros proyectos de ley en Bolivia, Ecuador y Chile relacionados con esta forma de violencia.

En los últimos años se han visto avances en varios países en la formación de órganos policiales especializados en ciberdelincuencia, que pueden investigar actos de violencia en línea contra las mujeres. La **Policía Federal de México** tiene una División Científica que investiga delitos cibernéticos nacionales y atiende casos de violencia en línea. Asimismo, la Fiscalía General de Justicia de la Ciudad de México creó recientemente la Unidad de Atención de Ciberdelitos de Violencia de Género[20], además de un portal gubernamental en línea para concientizar sobre el acoso cibernético. También hay organismos especializados en la **Policía Nacional de Colombia**, que tiene un Centro Cibernético Policial, y en **Brasil**, que cuenta con una **Oficina para la Represión de la Delincuencia Cibernética** en la Policía Federal (además de los departamentos de policía especializados de algunos estados). **Argentina** tiene una **División de Delitos Tecnológicos** en la Policía Federal; **Bolivia** tiene una **Agencia para el Desarrollo de la Sociedad de la Información,** que es el organismo principal de gestión de asuntos de seguridad, y **Paraguay** tiene una **Unidad Especializada de Delitos Informáticos.** Por último, el **Ministerio de la Mujer y Poblaciones Vulnerables de Perú** cuenta con una plataforma digital en la que se puede alertar sobre incidentes de acoso virtual[21].

[19] Orden jurídico. *Ficha Técnica Ley Olimpia.* Disponible en: http://ordenjuridico.gob.mx/violenciagenero/LEY%20OLIMPIA.pdf

[20] Alejandra Balandrán Olmedo (2020). "Atenderá FGJCDMX ciberdelitos de violencia de género". *Diario ContraRepública.* Disponible en: https://www.contrareplica.mx/nota-Atendera-FGJCDMX-ciberdelitos-de-violencia-de-genero202028854

[21] Ministerio de la Mujer y Poblaciones Vulnerables. *Ponte alerta ante el acoso virtual.* Disponible en: http://www.noalacosovirtual.pe/alerta.html

Para explorar más

La provisión de los siguientes recursos no representa un respaldo por parte de la OEA o de sus Estados Miembros a su contenido o a las organizaciones nombradas. Los recursos se presentan a modo de ejemplo de aquellas organizaciones, guías, herramientas, etcétera, que están disponibles en la región para que las personas lectoras puedan ampliar la información relacionada con la temática que aborda esta publicación.

Organizaciones, sitios de internet y líneas de apoyo:

Acoso.online (sitio que brinda herramientas e información útil en casos de publicación no consentida de imágenes y videos íntimos)
Asociación para el Progreso de las Comunicaciones (APC)
Ciberfeministas Guatemala
Ciber Civil Rights Initiative
Ciberseguras
Cl4ndestina (Brasil)
Coding Rights(Brasil)
Crash Override Network
Datos Protegidos (Chile)
Datysoc (Uruguay)
Derechos Digitales (América Latina)
Dominemos la Tecnología
Feminist Frequency
Frente Nacional para la Sororidad y Defensoras Digitales
Fundación Datos Protegidos
Fundación Activismo Feminista Digital
Fundación InternetBolivia.org (Bolivia)
Fundación Karisma (Colombia)
GenderIT.Org
HeartMob
Hiperderecho (Perú)
Internet es Nuestra
InternetLab (Brasil)
La <clika> libres en línea
Luchadoras (México)
MariaLab (Brasil)
Nodo Común
ONG Amaranta (Chile)
R3D (México)
Safernet (Brasil)
SocialTIC
SOS Digital (Bolivia)
TEDIC (Paraguay)
The Atlas of Online Harassment
Without My Consent

Guías:

A First Look at Digital Security. Access Now.

Alfabetización y Seguridad Digital: La Importancia de Mantenerse Seguro e Informado (2021). Organización de los Estados Americanos y Twitter.

Alfabetismo y Seguridad Digital. Mejores Prácticas en el uso de Twitter. Organización de los Estados Americanos, 2019.

Alza la voz y ten cuidado: Guía para protegerte del acoso online. *Feminist Frequency.*

Ciberseguridad de las mujeres durante la pandemia de COVID-19: Experiencias, riesgos y estrategias de autocuidado en la nueva normalidad digital. Organización de los Estados Americanos, 2021.

Cuidados durante la pandemia: ¿Cómo denunciar la violencia doméstica? Derechos Digitales y MariaLab.

Cuidar nuestr@ cuerp@ digital. Reflexiones de un equipo virtual. Fondo de Acción Urgente.

Data Detox x Youth. Tactical Tech.

Guía de Seguridad Digital para Feministas Autogestivas. *Hackblossom.*

Guía breve para la cobertura periodística de la violencia de género online (2020). Acoso.online.

Guía práctica para tratar casos de pornografía no consentida en recintos educacionales (2018). Acoso.online.

Netizens Online Security Guide.

Online Harassment Field Manual. (2019) PEN America.

Security in a Box (2020). Tactical Tech, Front Line Defenders.

Surveillance Self-Defense. Electronic Frontier Foundation.

Reportes:

Cyber Violence against Women and Girls. A World-Wide Wake-up Call. United Nations Broadband Commission for Digital Development (UNBC). Working Group on Broadband and Gender (2015).

(In)Seguras Online. Experiencias de niñas, adolescentes y jóvenes en torno al acoso online (2020). Plan Internacional.

Informe acerca de la violencia en línea contra las mujeres y las niñas desde la perspectiva de los derechos humanos (2018). Relatora Especial de las Naciones Unidas sobre la Violencia contra la Mujer, sus Causas y Consecuencias.

La ciberviolencia contra mujeres y niñas (2017). Instituto Europeo de la Igualdad de Género.

Online and ICT facilitated violence against women and girls during COVID-19 (2020). ONU Mujeres.

Reporte de la Situación de América Latina sobre la Violencia de Género Ejercida por Medios Electrónicos (2017). Paz Peña Ochoa (ed).

Ser periodista en Twitter. Violencia de Género digital en América Latina (2020). Sentiido-Colombia, Comunicación para la Igualdad y el Programa Internacional para el Desarrollo de la Comunicación de la Organización de las Naciones Unidas para la Educación, Ciencia y la Cultura (UNESCO).

Toxic Twitter - A Toxic Place for Women (2018). Amnistía Internacional.

Violencia en línea: La nueva línea de combate para las mujeres periodistas - #JournalistsToo (2021). UNESCO y el Centro Internacional para Periodistas (ICFJ).

Eventos TED y Documentales:

How Online Abuse of Women Has Spiraled Out of Control. Ashley Judd. TEDTalk, 2016.

Anita Sarkeesian at TEDxWomen 2012.

The problem with "Don't Feed the Trolls". Steph Guthrie, TEDxToronto.

Grooming, el acoso ¿virtual?. Sebastián Bortnik, TEDxRíodelaPlata, 2016.

Netizens. Cynthia Lowen, 2019.

Glosario de Términos

Aplicación (también llamada *app*). Es un programa informático creado para llevar a cabo o facilitar un conjunto de tareas determinadas (profesionales, de ocio, educativas, etc.) que se ejecuta en teléfonos inteligentes, tabletas u otros dispositivos móviles. Existen aplicaciones gratuitas y de paga, y por lo general se encuentran disponibles en plataformas de distribución específicas o a través de las compañías propietarias de los sistemas operativos de los dispositivos electrónicos.

***Blackout* o apagón de internet.** Una interrupción de la internet causada por un ataque a un sitio web, a un proveedor de servicio de internet (ISP) o al sistema de nombres de dominios de internet (DNS). También puede ser una interrupción debido a una configuración incorrecta de la infraestructura del servidor web.

Blog. Es un sitio web que permite la creación y publicación de artículos cortos sobre temas específicos o libres.

Brecha de género: Se refiere a cualquier disparidad entre la condición o posición de las mujeres y hombres en la sociedad (diferencias en el acceso a recursos, derechos y oportunidades).

Bot. Cuenta controlada por un algoritmo que usualmente se utiliza para coordinar una acción *online*.

Chat. Método de comunicación digital en tiempo real que se realiza entre varias personas usuarias cuyas computadoras están conectadas a una red.

***Cybermobs* o ciberturbas.** Acción de grupos organizados en línea que publican contenido ofensivo o destructivo de forma masiva con la intención de avergonzar a alguien o lograr el retiro de su perfil de redes sociales.

Cifrado de información. Es un proceso para convertir datos digitales en códigos, los cuales hacen la información ilegible excepto para la persona que posee la clave para descifrarlos.

Cortafuegos (*Firewall*). Sistema físico o digital que tiene el objetivo de permitir o prohibir el acceso desde o hacia una red a fin de asegurar que todas las comunicaciones entre la red e internet se realicen conforme a las políticas de seguridad de una organización o corporación.

Creepshot. Se refiere a una foto tomada por un hombre a una mujer o niña en público sin su consentimiento. Las fotos suelen centrarse en los glúteos, las piernas o el escote de la víctima.

Cyberflashing. Envío de fotografías obscenas a una mujer sin su consentimiento con el objetivo de molestarla, intimidarla o incomodarla.

***Deepfake* o video ultra falso.** Técnica de inteligencia artificial que permite editar videos falsos de personas que aparentemente son reales mediante el uso de algoritmos de aprendizaje y videos o imágenes ya existentes.

Denegación de servicio. Ciberataque que tiene por objeto saturar con peticiones de servicio a un servidor a fin de impedir que personas usuarias legítimas puedan utilizarlo. Un método más sofisticado es el ataque de Denegación de Servicio Distribuido (DDoS), mediante el cual las peticiones son enviadas de forma coordinada entre varios equipos.

Discurso de odio. Es el uso de un lenguaje que denigra, insulta, amenaza o ataca a una persona a causa de su identidad y/u otras características, como su orientación sexual o discapacidad.

Discriminación por razón de género. Toda distinción basada en el sexo que tenga por objeto o por resultado menoscabar o anular el reconocimiento, goce o ejercicio por la mujer, independientemente de su estado civil, sobre la base de la igualdad del hombre y la mujer, de los derechos humanos y las libertades fundamentales en las esferas política, económica, social, cultural y civil o en cualquier otra esfera [Fuente: Artículo 1 de la Convención sobre la Eliminación de todas las Formas de Discriminación contra la Mujer].

Downblousing. Registro sin consentimiento de fotografías tomadas por arriba de la blusa de una mujer.

Doxxing o doxing. El término proviene de la frase en inglés *dropping docs*, y consiste en en la extracción y la publicación en línea no autorizadas de información personal.

Emoji. Pequeña imagen o icono digital que se usa en las comunicaciones electrónicas para representar una emoción, un objeto, una idea, etc.

Estereotipos de género. Es una opinión o un prejuicio generalizado acerca de atributos o características que hombres y mujeres poseen o deberían poseer o de las funciones sociales que ambos desempeñan o deberían desempeñar [Fuente: OHCHR, *Estereotipos de género y su utilización*].

Gamertag. Identificador de personas que juegan y comparten contenido en la comunidad de la plataforma digital de Microsoft Xbox Live. Se crea a partir de un alias, un avatar o una imagen e información sobre las preferencias de la o el jugador.

Gaslighting. Es una forma de abuso psicológico realizado mediante la manipulación de la realidad de la víctima, con lo cual se busca que se cuestione su cordura, su memoria o su percepción.

Geolocalización. Es la capacidad para obtener la ubicación geográfica real de un objeto, como un radar, un teléfono móvil o un ordenador conectado a internet.

Género. Se refiere a los roles, comportamientos, actividades, y atributos que una sociedad determinada en una época determinada considera apropiados para hombres y mujeres. El género también hace referencia a las relaciones entre mujeres y las relaciones entre hombres. Estos atributos, oportunidades y relaciones son construidos socialmente y aprendidos a través del proceso de socialización [Fuente: ONU Mujeres, *OSAGI Gender Mainstreaming - Concepts and definitions*].

***Grooming* o ciberengaño pederasta.** Son actos deliberados de un adulto para acercarse a una persona menor de edad con el objetivo de establecer una relación y un control emocional que le permita cometer abusos sexuales, entablar relaciones virtuales, obtener pornografía infantil o traficar a la o al menor de edad.

Hackeo. Uso de técnicas y procedimientos por un *hacker* para introducirse sin autorización en sistemas informáticos ajenos con el fin de manipularlos o de obtener información o por diversión. El *cracking* es una práctica relacionada con el *hackeo*, pero implica entrar en sistemas ajenos con fines delictivos para violar la intimidad de la persona afectada o la confidencialidad de la información o dañar la información o los soportes físicos.

Hacker. Persona que obtiene acceso no autorizado a un sistema informático.

***Hashtag* o etiqueta.** Cadena de caracteres que inician con el símbolo #. Se utiliza en redes sociales para indicar la temática de una conversación o de un mensaje. Además, permite la creación automática de un hipervínculo que brinda acceso a todos los contenidos que incluyan el *hashtag* en cuestión.

HTTPS. Corresponde a las siglas en inglés de *Hypertext Transfer Protocol Secure* y consiste en un protocolo de red destinado a la transferencia segura de datos cifrados.

Internet de las Cosas (*Internet of Things* o *IoT* por sus siglas en inglés). Se refiere a la red de dispositivos y objetos cotidianos conectados a la internet que pueden compartir datos entre sí.

Igualdad de género. Se refiere a la igualdad de derechos, responsabilidades y oportunidades de las mujeres y los hombres y de las niñas y los niños [Fuente: ONU Mujeres, *OSAGI Gender Mainstreaming - Concepts and definitions*].

***Keylogger* o registrador de teclas.** Es un *software* malicioso que se coloca entre el teclado y el sistema operativo para interceptar y registrar información de cada tecla pulsada en el dispositivo sin que la persona usuaria lo sepa.

Malware o programa malicioso. El término nace de la unión de las palabras en inglés *malicious software* y hace referencia a un tipo de *software* que tiene como objetivo infiltrarse y/o dañar un sistema de información sin el consentimiento de la persona usuaria.

Metadatos. Son datos sobre datos, es decir, es información que se usa para describir los datos contenidos en un archivo, documento, fotografía, una página web, etc.

Nube. Designa la red mundial de servidores diseñados para almacenar y administrar datos, ejecutar aplicaciones o entregar contenido o servicios.

Outing. Revelación en línea de la identidad o preferencia sexual de una persona.

Packs. Conjunto de imágenes de mujeres de naturaleza íntima o sexual obtenidas y/o distribuidas sin su consentimiento.

Perspectiva de género. Mecanismo de análisis que consiste en observar el impacto del género en las oportunidades, roles e interacciones sociales de las personas [Fuente: ONU Mujeres, *OSAGI Gender Mainstreaming - Concepts and definitions*].

***Phishing* o ataque de pesca de información.** Es una estafa cometida a través de una comunicación electrónica engañosa y aparentemente oficial (correo electrónico, mensaje de texto o telefónicamente) mediante la cual el estafador o *phisher* suplanta la personalidad de una persona o empresa de confianza para que la persona receptora facilite información confidencial (contraseñas, datos bancarios, etc.). Se denomina *smishing* cuando la estafa se realiza vía SMS y *vishing* cuando se realiza recreando una voz automatizada.

Pornovenganza. Término utilizado de forma incorrecta para referirse a la distribución no consensuada de imágenes o videos íntimos.

***Raiding* o troleo colectivo.** Ataque coordinado de una gran cantidad de cuentas en contra de una persona usuaria específica para producir un impacto significativo.

Red Privada Virtual. También referida como VPN por sus siglas en inglés (*Virtual Private Network*), es una tecnología de red de ordenadores que establece una extensión segura de una red de área local (LAN) sobre una red pública o no controlada, permitiendo que el ordenador en la red envíe y reciba datos sobre redes públicas como si fuera una red privada (consiguiendo que esta conexión sea segura gracias al cifrado de la información).

Red Social. Servicio de la sociedad de la información que ofrece a las persona usuarias una plataforma de comunicación a través de internet para que generen un perfil con sus datos personales, facilitando la creación de comunidades con base en criterios comunes y permitiendo la comunicación, de modo que las personas usuarias pueden interactuar mediante mensajes, compartir información, imágenes o videos, permitiendo que estas publicaciones sean accesibles de forma inmediata por todas las personas de un grupo [Fuente: Real Academia Española].

Roles de género. Normas sociales y de conducta que, dentro de una cultura específica, son ampliamente aceptadas como socialmente apropiadas para las personas de un sexo específico. Suelen determinar las responsabilidades y tareas tradicionalmente asignadas a hombres, mujeres, niños y niñas [Fuente: UNICEF, UNFPA, PNUD, ONU Mujeres. *Gender Equality, UN Coherence and you*].

Sexo (biológico). Se refiere a las características biológicas que definen a los seres humanos como mujeres y hombres.

***Sexting* o sexteo.** Es una práctica que implica la generación e intercambio de material sexualmente explícito entre dos personas. Puede incluir la creación y envío de imágenes de forma consensuada o la creación consensuada de imágenes que se distribuyen sin consentimiento.

Sextorsión. Consiste en amenazar a una persona con difundir imágenes o videos íntimos con la finalidad de obtener más material sobre actos sexuales explícitos, mantener relaciones sexuales u obtener dinero.

Slutshaming. Es una forma de violencia que consiste en señalar públicamente a una mujer por su supuesta actividad sexual con el fin de avergonzarla, dañar su reputación y regular su sexualidad. Puede implicar el uso de fotografías y/o videos y lenguaje denigrante.

Sockpuppet o cuenta marioneta: Cuentas falsas no automatizadas que buscan pasar como usuarios reales para desinformar o difundir contenido sesgado sobre temas específicos.

Software. Conjunto de programas, instrucciones y reglas informáticas que permiten a los dispositivos electrónicos realizar determinadas tareas.

***Spyware* o *software* espía.** Un tipo de programa maligno que infecta un dispositivo y graba secretamente y sin consentimiento datos de navegación, información personal, ubicación del dispositivo, registro de llamadas o mensajes, entre otros datos personales.

Trending topic. Hace referencia a la palabra o frases más repetidas en redes sociales en un momento determinado.

***Troll* o trol.** Persona con identidad desconocida que publica en línea mensajes con la intención de molestar, provocar una respuesta emocional por parte de las personas usuarias o alterar las conversaciones en línea.

Troleo de género. Publicación de mensajes, imágenes o videos, así como la creación de *hashtags* (etiquetas), con el propósito de molestar a mujeres y niñas o incitar a la violencia contra ellas.

Upskirting. Registro sin consentimiento de fotografías tomadas por debajo de la falda de una mujer o niña.

URL. Por las siglas en inglés *Uniform Resource Locator*, se refiere a la dirección específica que se asigna a cada uno de los recursos disponibles en la red (páginas, sitios, documentos) con la finalidad de que puedan ser localizados o identificados.

Violencia contra la mujer. 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 [Fuente: Artículo 1 de la Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia contra la Mujer].

Violencia de género en línea o ciberviolencia de género contra la mujer. Todo acto de violencia por razón de género contra la mujer cometido, con la asistencia, en parte o en su totalidad, del uso de las Tecnologías de la Información y la Comunicación, o agravado por este, como los teléfonos móviles y los teléfonos inteligentes, internet, plataformas de medios sociales o correo electrónico, dirigida contra una mujer porque es mujer o que la afecta en forma desproporcionada [Fuente: Relatora Especial sobre Violencia de la Organización de las Naciones Unidas].

Virus. Es un programa informático auto propagado que tiene por objeto alterar el funcionamiento normal de un dispositivo electrónico. Los virus se diferencian de otros tipos de programa maligno en que se replican automáticamente, es decir, son capaces de copiarse de un archivo o un ordenador a otro sin el consentimiento de la persona usuaria.

Wi-Fi. Es una red de dispositivos inalámbricos interconectados entre sí y generalmente también conectados a la internet a través de un punto de acceso inalámbrico.

Bibliografía

Abdul Aziz, Z (2017). Due Diligence and Accountability for Online Violence against Women. APC Issue Papers, Consultado el 9 de septiembre de 2020.

Agencia de los Derechos Fundamentales de la Unión Europea (FRA) (2014). Violencia de género contra las mujeres: una encuesta a escala de la UE. Consultado el 9 de septiembre de 2020.

Amnesty International (2018). Toxic Twitter-A Toxic Place for Women. Consultado el 9 de septiembre de 2020.

--- (2017). *Amnistía revela alarmante impacto de los abusos contra las mujeres en Internet.* Consultado el 9 de septiembre de 2020.

Amnistía Internacional (2019). Corazones Verdes. Violencia online contra las mujeres durante el debate por la legalización del aborto en Argentina. Disponible en: https://amnistia.org.ar/corazonesverdes/files/2019/11/corazones_verdes_violencia_online.pdf

Association of Progressive Communications (APC) (2017). *Online gender-based violence: A submission from the Association for Progressive Communications to the United Nations Special Rapporteur on violence against women, its causes and consequences.*

--- (2015). Briefing paper on VAW. APC Women's Rights Programme. Consultado el 9 de septiembre de 2020.

Barrera, L. (coord) (2017). *La Violencia en Línea contra las Mujeres en México.* Informe para la Relatora Especial sobre la violencia contra la mujer. Luchadoras, México.

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

Comité para la Eliminación de la Discriminación contra la Mujer de las Naciones Unidas (Comité CEDAW) (2017). CEDAW/C/GC/35. Recomendación general núm. 35 sobre la violencia por razón de género contra la mujer, por la que se actualiza la recomendación general núm. 19. Consultado el 9 de septiembre de 2020.

--- (1992). A/47/38. Recomendación General No. 19. La Violencia contra la Mujer. Consultado el 9 de septiembre de 2020.

Comisión Interamericana de Mujeres (CIM) (2020). COVID-19 en la vida de las mujeres. Razones para reconocer los impactos diferenciados. Consultado el 9 de septiembre de 2020.

Cuellar, L y Sandra Chaher (2020). *Ser periodista en Twitter. Violencia de género digital en América Latina.* Fundación Sentiido, Comunicación para la Igualdad Ediciones, UNESCO.

Deeptrace (2019). The State of Deepfakes: Landscape, Threats and Impact. Consultado el 9 de septiembre de 2020.

Derechos Digitales América Latina (2020). *COVID-10 and the increase of domestic violence against women in Latin America: A digital rights perspective.* Documento presentado por Derechos Digitales a la Relatora Especial de las Naciones Unidas sobre la violencia contra la mujer, sus causas y consecuencias.

Dragiewicz, H., Woodlock et. al (2019) *Domestic violence and communication technology: Survivor experiences of intrusion, surveillance, and identity crime.* Brisbane: Queensland University of Technology.

Edwards, A. (2010). "Feminist Theories on International Law and Human Rights". En *Violence against Women under International Human Rights Law*, 36-87. Cambridge: Cambridge University Press.

Fanti K., A. G. Demetriou, y V. Hawa. (2012). "A longitudinal study of cyberbullying: Examining risk and protective factors". En *European Journal of Developmental Psychology*, Vol. 9(2), 168-181.

Federal Bureau of Investigation. Internet Crime Complaint Center (FBI-ICC) (2018). Internet Crime Report. Consultado el 9 de septiembre de 2020.

Fondo de las Naciones Unidas para la Infancia (UNICEF) (2017). Access to the Internet and Digital Literacy. Consultado el 9 de septiembre de 2020.

Freed, D., J, Palmer, D. Minchala, et al. (2017). "Digital technologies and intimate partner violence: a qualitative analysis with multiple stakeholders". En *Proceedings ACM Human-Computer Interaction*, Vol. 1, 46:1- 46:22.

Goldsman, F. y G. Natansohn (2020). *Cuidados durante la pandemia: ¿Cómo denunciar la violencia Doméstica?* Derechos Digitales y María Lab.

Henry, N. y A. Powell (2018). "Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research". En *Trauma, Violence, & Abuse*, Vol. 19 (2), 195-208.

Henry, N. y A. Powell (2017). "Sexual Violence and Harassment in the Digital Era". En Antje Deckert y Rick Sarre (eds.). *The Palgrave Handbook of Australian and New Zealand Criminology, Crime and Justice.* Palgrave Macmillan.

Henry, N. y A. Powell (2016). "Sexual Violence in the Digital Age: The Scope and Limits of Criminal Law". En *Social & Legal Studies*, Vol. 25 (4), 397-418.

Henry, N., A. Powell y F., Asher (2018). *"AI can now create fake porn, making revenge porn even more complicated"*. En *The Conversation.*

--- (2017). Not just "revenge pornography": Australians' experiences of image-based abuse: A summary report. Gender Violence and Abuse Research Alliance (GeVARA). Centre for Global Research, Centre for Applied Social Research.

Harris, B. (2018). "Spacelessness, spatiality and intimate partner violence: Technology-facilitated abuse, stalking and justice". En K. Fitz-Gibbon, S. Walklate, J. McCullough, y J. Maher (eds.), *Intimate partner violence, risk and security: Securing women's lives in a global world* (pp. 52–70). Londres: Routledge.

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

Hinson L., J. Mueller, L. O'Brienn-Milne, N. Wandera (2018). *Technology-facilitated gender-based-violence: What is it, and how to we measure it?* Washington D.C., International Center for Research on Women.

Interagency Working Group (2016). "Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse". En *ECPAT International and ECPAT Luxembourg*, Luxemburgo. Consultado el 9 de septiembre de 2020.

Internet Governance Forum (IGF) (2015). 2015: Best Practice Forum (BPF) on Online Abuse and Gender-Based Violence against Women. Consultado el 9 de septiembre de 2020.

Instituto Europeo de la Igualdad de Género (EIGE) (2017). La ciberviolencia contra mujeres y niñas. Consultado el 9 de septiembre de 2020.

Jane, E. (2017). *Misogyny Online.* A Short (and Brutish) History. Londres: Sage Publications.

Jane E. (2016). "Online Misogyny and Feminist Digilantism". En *Continuum. Journal of Media & Cultural Studies*, Vol. 30 (3), 284-297.

Kelly, L. (1988) *Surviving Sexual Violence.* Cambridge: Polity.

Knight, W. (2018). "The Defense Department has produced the first tools for catching deepfakes". En *MIT Technology Review.* Consultado el 9 de septiembre de 2020.

Kwon, M., Y. S. Seo, S. S. Dickerson, E. Park, y J. A. Livingston (2019). "Cyber Victimization and Depressive Symptoms: A Mediation Model Involving Sleep Quality". En *Sleep*, 42(Supplement_1), A322–A322.

Qing Li (2006). "Cyberbullying in schools: a research of gender differences". En *School Psychology International*, Vol. 27(2), 157-170.

Mantilla. K. (2013). "Gendertrolling: misogyny adapts to new media". En *Feminist Studies*, Vol. 39(2), 563–570.

Maras, M. (2016). *Cybercriminology*. Oxford University Press.

Maras, M., y A.Alexandrou (2018). "Determining Authenticity of Video Evidence in the Age of Artificial Intelligence and in the Wake of Deepfake Videos". En *International Journal of Evidence and Proof*, Vol. 23(3), 255-262.

Mecanismo de Seguimiento de la Convención de Belém do Pará (MESECVI). Comisión Interamericana de Mujeres (2017). Tercer Informe Hemisférico sobre la Implementación de la Convención de Belém do Pará. Consultado el 9 de septiembre de 2020.

Salter M., T. Crofts y M. Lee (2013). "Beyond Criminalisation and Responsibilisation: Sexting, Gender and Young People". En *Current Issues in Criminal Justice*, Vol. 24 (3), 301-316.

Navarro, J. y J. L. Jasinski (2012). "Going Cyber: Using Routine Activities Theory to Predict Cyberbullying Experiences". En *Sociological Spectrum*, Vol. 32(1), 81-94.

Neris, N., J. Ruiz y M. Valente (2018). Enfrentando Disseminação Não Consentida de Imagens Íntimas: Uma análise comparada. InternetLab. Consultado el 9 de septiembre de 2020.

Oficina de Naciones Unidas para la Droga y el Delito (UNODC) (2015). Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children. Consultado el 9 de septiembre de 2020.

--- (2019). University Module Series. Cybercrime. Module 12. Interpersonal Crime.
Organización de las Naciones Unidas. Asamblea General (2018). Intensificación de los esfuerzos para prevenir y eliminar todas las formas de violencia contra las mujeres y las niñas: el acoso sexual. A/C.3/73/L.21/Rev.1. Consultado el 9 de septiembre de 2020.

---. Consejo de Derechos Humanos (2018). Acelerar los esfuerzos para eliminar la violencia contra las mujeres y las niñas: prevención de la violencia contra las mujeres y las niñas en los contextos digitales. A/HRC/38/L.6. Consultado el 9 de septiembre de 2020.

---. Comisión de la Banda Ancha para el Desarrollo Sostenible (UNBC-UN) (2015). Working Group on Broadband and Gender. Cyber Violence against Women and Girls. A World-Wide Wake-up Call. Consultado el 9 de septiembre de 2020.

Organización de Estados Americanos (OEA) (2019). Media Literacy and Digital Security: Twitter Best Practices. Consultado el 9 de septiembre de 2020.

Peña Ochoa, P. (ed) (2017). *Reporte de la Situación de América Latina sobre la Violencia de Género Ejercida por Medios Electrónicos.* Presentación para la Relatora Especial sobre la violencia contra la mujer.

Pew Research Center (2014). Online Harassment 2014. Consultado el 9 de septiembre de 2020.

--- (2017). Online Harassment 2017. Consultado el 9 de septiembre de 2020.

Powell, A., N. Henry, y F. Asher (2018). "Image-based Sexual Abuse". En Walter DeKeseredy and Molly Dragiewicz (eds.) *Handbook of Critical Criminology.* Nueva York: Routledge.

Relatora Especial de las Naciones Unidas sobre la Violencia contra la Mujer, sus Causas y Consecuencias (REVM-ONU) (2018). A/HRC/38/47. *Informe acerca de la violencia en línea contra las mujeres y las niñas desde la perspectiva de los derechos humanos.* Consultado el 9 de septiembre de 2020. https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session38/Documents/A_HRC_38_47_EN.docx

Relator Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (RELE) (2018). *Mujeres periodistas y libertad de expresión: Discriminación y violencia basada en el género contra las mujeres periodistas por el ejercicio de su profesión* (OEA/Ser.L/V/II), párr. 48. Disponible en: http://www.oas.org/es/cidh/expresion/docs/informes/MujeresPeriodistas.pdf

Reyns, Bradford, Billy Henson y Bonnie S. Fisher (2011). "Being pursued online. Applying Cyberlifestyle-Routine activities theory to cyberstalking victimization". En *Criminal Justice and Behavior*, Vol. 38(11), 1149-1169.

Salter, M. y T. Crofts y M. Lee (2013). "Beyond Criminalisation and Responsibilisation: Sexting, Gender and Young People". En *Current Issues in Criminal Justice*, Sydney Law School Research Paper No. 13/38, Vol. 24(3), 301-316.

Segrave, M., y L. Vitis (2017), *Gender, Technology and Violence.* Oxon y Nueva York: Routledge.

Smith, Peter K. (2012). "Cyberbullying and cyber aggression". En S.R. Jimerson, A.B. Nickerson, M.J. Mayer, y M.J. Furlong. (eds). *Handbook of school violence and school safety: International research and practice* (pp. 93-103). Routledge.

Van Der Wilk, A. (2018). *Cyber violence and hate speech online against women.* Estudio encargado por el Departamento Temático de Derechos de los Ciudadanos y Asuntos Constitucionales del Parlamento Europeo. Bruselas: Parlamento Europeo.

Vela, E. y E. Smith. "La violencia de género en México y las tecnologías de la información". En *Internet en México: Derechos Humanos en el entorno digital.* Ed. Juan Carlos Lara. México: Derechos Digitales, 2016. Consultado el 9 de septiembre de 2020.

Walker, Shelley, Sanci, Lena y Temple-Smith Meredith (2013). "Sexting: Young women's and men's views on its nature and origins". En *Journal of Adolescent Health*, Vol. 52, 697-701.

Web Foundation (2018a). Advancing Women's Rights Online: Gaps and Opportunities in Research and Advocacy. Consultado el 9 de septiembre de 2020.

Web Foundation (2018b). *Measuring the digital divide: Why we should be using a women-centered analysis.* Consultado el 9 de septiembre de 2020.

Women's Aid (2014). *Virtual World, Real Fear. Women's Aid report into online abuse, harassment and stalking.*

Women's Media Center (2019). *Online Abuse 101.* Consultado el 9 de septiembre de 2020,

Woodlock D (2017). "The abuse of technology in domestic violence and stalking". En *Violence Against Women*, Vol. 23(5, 584-602.

La violencia de género en línea contra las mujeres y niñas

Guía de conceptos básicos

ISBN 978-0-8270-7306-7

OEA | CICTE

OEA | CIM | MESECVI