Violencia Basada en Género facilitada por la tecnología

Hacer que todos los espacios sean seguros

División Técnica
Diciembre de 2021

Violencia Basada en Género facilitada por la tecnología

Hacer que todos los espacios sean seguros

Diciembre de 2021

Agradecimientos

A medida que el mundo sigue evolucionando y expandiéndose en el uso de la tecnología y las plataformas, también lo hace la expansión de los espacios a través de los cuales se puede perpetrar la violencia.

Esto se puso de manifiesto durante la pandemia de COVID-19, en la que los esfuerzos de contención redujeron el acceso a la información y los servicios, impulsando un mayor uso de la tecnología y los espacios en línea. Este documento sirve como señal de alarma para que la comunidad internacional, los movimientos digitales y feministas, las empresas privadas de tecnología y los gobiernos nacionales actúen al unísono para acabar con la creciente ola de violencia basada en género facilitada por la tecnología.

El Fondo de Población de las Naciones Unidas - UNFPA, desea agradecer la contribución de su valioso tiempo y experiencia en los debates y la revisión técnica: A la Dra. Suzie Dunn, Profesora Adjunta de Derecho y Tecnología en la Facultad de Derecho Schulich de la Universidad de Dalhousie; a Sophie Read-Hamilton, Consultora Independiente de VBG y Chandra Pauline Daniel Ph.D. del Programa de Doctorado en Salud Pública-Política y Gestión en Salud, New York Medical College; al Pasante de Análisis de Resultados del Plan Estratégico - PSIPB-División de Política y Estrategia, UNFPA.

Este informe ha sido elaborado por la División Técnica del UNFPA, Subdivisión de Género y Derechos Humanos, bajo la dirección técnica de Alexandra Robinson. Las coautoras del documento son Alexandra Robinson y Nora Piay-Fernández, con la revisión de Sarah Baird, Mar Jubero, Dawn Minott y Jude Larnerd.

Contenido

Parte 1

¿Qué es la VBG-FT?

Definición, Prevalencia e Impacto

Antecedentes

La aparición de la tecnología y los espacios digitales, y la creciente dependencia de ellos, es una megatendencia mundial[1], un fenómeno universal que está configurando nuestro mundo actual. La digitalización está impulsando cambios estructurales en la forma en que las personas se comunican, trabajan, aprenden, producen y consumen. La innovación tecnológica y la digitalización están abriendo una ventana de oportunidades para el desarrollo sostenible, en un momento en que muchos aspectos de la vida humana se están transformando radicalmente.[2] La tecnología tiene el potencial de fomentar el crecimiento económico; ampliar el acceso a la educación, la información y el conocimiento; y dar voz y poder a las personas dejadas atrás y a aquellos cuyas voces no se oían tradicionalmente, fomentando así la participación en la vida pública y los procesos democráticos.

Sin embargo, aunque la digitalización del mundo representa una gran oportunidad, también es un espacio a través del cual pueden perpetrarse daños. Las investigaciones indican que al menos el 38% de las mujeres de todo el mundo han experimentado personalmente violencia en línea y que esta tasa va en aumento.[3] La violencia basada en género facilitada por la tecnología (VBG-FT) está dirigida a todas las mujeres que utilizan la tecnología, incluidas las mujeres cis y trans y las personas que se presentan como femeninas, no binarias o de género diverso.[4] Ciertos grupos de mujeres corren un mayor riesgo debido a lo que hacen, quiénes son o si acceden a cierta información y servicios. Esto incluye, por ejemplo, a las periodistas, las políticas, las activistas y feministas, las académicas y las jóvenes.[5] De las adolescentes que tienen acceso a las tecnologías digitales, el 64% son grandes usuarias y son especialmente vulnerables a la VBG-FT.[6] La violencia contra las mujeres y las niñas es más frecuente si tienen una discapacidad, son racializadas, LGBTQIA+, están en desventaja socioeconómica y/o son activas en la vida política.[7]

En palabras del Women's Legal Education and Action Fund:

> [La ubicuidad de Internet significa que la VBG-FT puede llegar a ser omnipresente e implacable, infiltrándose en los espacios físicos más íntimos de la víctima, como su casa o su dormitorio. Los usuarios que ejercen la VBG-FT también pueden aprovechar sus propias redes sociales y las de las personas que sufren violencia para fomentar el abuso, reclutando a otros para que compartan, consciente o inconscientemente, material abusivo, y contaminando los propios espacios y comunidades en línea de las víctimas. La permanencia en línea del material abusivo -que es extremadamente difícil de erradicar por completo una vez compartido en línea- también garantiza la revictimización continua, lo que provoca daños duraderos, tanto psicológicos como de otro tipo.[8]

Además, la VBG-FT puede adoptar muchas formas y se comete en un continuo. Es decir, se comete como parte de un patrón de violencia perpetrada tanto en línea como fuera de línea.[9]

Ya no es negociable el abordaje de la VBG-FT, como un área crítica de creciente preocupación. Garantizar que todo el mundo pueda participar libremente en línea y sin miedo a la violencia y el abuso es vital para garantizar que las mujeres puedan ejercer efectivamente su derecho a la libertad de expresión. El Consejo de Derechos Humanos de las Naciones Unidas declaró que "los mismos derechos que tienen fuera de línea las personas deben protegerse en línea, en particular la libertad de expresión, lo que es aplicable independientemente de las fronteras y por conducto de cualquier medio de su propia elección, de conformidad con el artículo 19 de la Declaración Universal de Derechos Humanos y el Pacto Internacional de Derechos Civiles y Políticos".[10]

Más concretamente, el principio de que los derechos humanos y los derechos de la mujer protegidos fuera de línea deben protegerse también en línea, debe integrar plenamente el derecho a vivir libre de nuevas formas de violencia contra la mujer en línea y facilitada por las tecnologías de la información y la comunicación, respetando al mismo tiempo el derecho a la libertad de expresión y el derecho a la intimidad y a la protección de datos.[11]

El uso de la tecnología y de los espacios en línea debe servir como herramienta para acelerar la consecución de la igualdad de género y el empoderamiento de las mujeres, en lugar de ser una herramienta de subyugación, perpetración de la violencia y silenciamiento de las mujeres en toda su diversidad.

Definición de la VBG -FT

Existe una falta de consenso a nivel mundial sobre la definición de la violencia perpetrada mediante el uso de la tecnología y cometida a través de espacios en línea y digitales.[12] Una definición bien establecida, aceptada internacionalmente y estandarizada de la VBG-FT es fundamental para proporcionar una comprensión común que permita una medición estandarizada y unas normas mínimas para la respuesta y la prevención.

Para contribuir a superar esta brecha crítica en el conocimiento, UNFPA ha revisado los términos y definiciones publicados por organizaciones internacionales, académicos y organizaciones de la sociedad civil en los últimos cinco años y ha propuesto una nueva definición de trabajo. Basándose en estas definiciones y en su complementariedad, UNFPA propone adaptar el término abuso facilitado por la tecnología al término más amplio de VBG -FT, que se define de la siguiente manera:

> Un acto de violencia perpetrado por uno o más individuos que se comete, aporta, agrava o amplifica en parte o totalmente mediante el uso de tecnologías de la información y la comunicación o medios digitales,[13] contra una persona por razón de su género.

Se ha elegido esta amplia definición de trabajo porque (1) pone de relieve la violencia basada en el género y (2) incluye las circunstancias y formas en las que la tecnología puede utilizarse para perpetrar la violencia. Esta definición amplia e inclusiva engloba las pautas existentes de violencia, acoso y abuso, así como las nuevas formas de abuso, como el abuso basado en la imagen (IBA, por sus siglas en inglés). Además, esta terminología permite diferenciar "*violencia en línea*" o "*violencia digital*", como la violencia perpetrada contra las mujeres en espacios en línea o a través de medios digitales, de la "*violencia facilitada por la tecnología*", perpetrada por cualquier tipo de medio tecnológico, tecnología de la información y las comunicaciones y medios digitales, incluidos teléfonos, dispositivos de seguimiento del Sistema de Posicionamiento Global (GPS), drones y dispositivos de grabación no conectados a Internet.

Características de la VBG-FT

La VBG-FT comparte características comunes con otras formas de violencia basada en género:

- Ocurre en todas las sociedades del mundo.
- Se basa en el género y está arraigada en la desigualdad de género, por lo que afecta de manera desproporcionada a mujeres y niñas en toda su diversidad.
- Puede tener graves repercusiones en la salud, bienestar y vida de las personas sobrevivientes.

naturaleza digital

La VBG-FT también tiene características distintivas relacionadas con su naturaleza digital:[14]

Anonimato
El perpetrador o agresor puede permanecer en el anonimato.

Acción a distancia
Puede perpetrarse a distancia, desde cualquier lugar del mundo y sin contacto personal o físico con la persona sobreviviente.

Accesibilidad y asequibilidad
Es accesible y asequible para los perpetradores, ya que las tecnologías de la información y la comunicación han reducido el costo y la dificultad de producir y distribuir información a gran escala.

Propagación
Es constante y se propaga fácilmente por Internet, lo que vuelve a revictimizar a las personas sobrevivientes.
La facilidad, eficacia y asequibilidad de automatizar y multiplicar los casos de abuso contra un grupo o individuo concreto significa que es una forma eficaz de violencia para causar daño.

Impunidad
A menudo se perpetra con impunidad. Dado que la VBG-FT puede cometerse de forma anónima y a distancia, existen dificultades en la aplicación de la ley en distintos países y jurisdicciones que limitan la capacidad de los sistemas judiciales para hacer que los agresores respondan por sus actos.

Automatización
Puede ser automático y fácil de perpetrar, y permite a los agresores controlar los movimientos de las mujeres, vigilar su actividad en línea y distribuir imágenes o información, entre otras acciones abusivas perjudiciales, con tiempo y esfuerzo limitados.

Colectividad
Puede ser organizada colectivamente y perpetrada por un gran número de individuos.

Normalización de la violencia
La VBG-FT contribuye a la normalización de la violencia contra las mujeres y las niñas. La violencia física contra las mujeres suele estar normalizada y justificada, sobre todo por las propias mujeres. De hecho, en 49 países de ingresos bajos y medios, el 41% de las mujeres y el 32% de los hombres justifican la violencia física doméstica en al menos una circunstancia.[15] Es probable que esta normalización de la violencia se exacerbe en el espacio digital, y que la VBG-FT se perciba como menos grave, dañina o peligrosa para las personas sobrevivientes.

Perpetuidad
Puede cometerse a perpetuidad, ya que es probable que las imágenes y los materiales digitales utilizados para perpetrar abusos existan indefinidamente o durante largos periodos de tiempo.

Formas de VBG-FT

La VBG-FT "se lleva a cabo a través de texto, imágenes y vigilancia y seguimiento no deseados o mejorados digitalmente, utilizando una variedad de dispositivos y plataformas, desde herramientas digitales básicas, como mensajes de texto, correo electrónico y redes sociales, hasta tecnologías más avanzadas como la inteligencia artificial (IA), el seguimiento por GPS y drones".[16] A medida que se dispone de nuevas tecnologías y espacios digitales, surgen nuevas formas de VBG-FT, como el uso de la IA para la IBA o el acoso mediante rastreo por GPS de los dispositivos de telefonía móvil.[17] Al mismo tiempo, las viejas tecnologías se utilizan para perpetrar nuevas formas de violencia. Por ejemplo, en el contexto de las relaciones íntimas abusivas, los perpetradores utilizan transferencias bancarias por Internet para enviar mensajes de acoso a las personas sobrevivientes.[18]

Algunas de las formas más comunes de VBG -FT son, entre otras:[19]

Acoso en línea, incluido el acoso sexual y por razón de género en línea

El acoso en línea es el uso de la tecnología para contactar repetidamente, molestar, amenazar o asustar a otra persona. El acoso en línea es un comportamiento continuo en el tiempo más que un incidente aislado.[20] El acoso en línea puede ser perpetrado por un solo individuo o por grupos de individuos (*mobbing*), normalmente redes de perpetradores hombres que atacan a mujeres y minorías.[21] Cuando el acoso en línea se perpetra por motivos de género, sexualidad u orientación sexual de la persona sobreviviente, constituye una forma de VBG-FT .[22] El acoso sexual en línea es una forma específica de acoso que puede implicar atención sexual no deseada y coacción sexual.[23] También se ha definido como "cualquier comportamiento sexual no deseado a través de medios electrónicos y puede incluir insinuación sexual no deseada; peticiones no deseadas de hablar sobre sexo; peticiones no deseadas de hacer algo sexual en línea o en persona; recibir mensajes e imágenes sexuales no deseadas; compartir mensajes e imágenes sexuales sin permiso; y revelar información personal o de identidad sobre una persona en línea".[24]

1

Ciberacecho, rastreo o persecución y cibervigilancia obsesiva

2

El ciberacecho es "el uso de la tecnología para acechar y vigilar las actividades y comportamientos de otra persona en tiempo real o históricamente".[25] El ciberacecho suele considerarse una extensión del acoso convencional, mediante el uso de herramientas tecnológicas, e implica una serie de comportamientos no deseados, repetitivos, intrusivos, amenazantes y acosadores, que en algunos casos se consideran relativamente normales una práctica relacional o de citas. Algunos estudiosos utilizan el término "persecución ciberobsesiva" para referirse a la "búsqueda no deseada de intimidad a través de una invasión repetida del sentido de intimidad física o simbólica de una persona, utilizando medios digitales o en línea" y el ciberacecho es una forma grave de persecución y cibervigilancia obsesiva, que puede estar motivada por el control o la destrucción de las relaciones y provocar que la persona sobreviviente se sienta amenazada.[26]

El ciberacecho consiste, por ejemplo, en vigilar o rastrear la ubicación o las actividades de una persona utilizando localizadores GPS, programas espía[27], cámaras y micrófonos, aplicaciones de citas basadas en la ubicación, consultas de historiales de correo electrónico, llamadas o mensajes, así como el monitoreo de los perfiles de redes sociales de una persona.[28]

IBA

3

El abuso basado en la imagen (IBA, por sus siglas en inglés) consiste en "utilizar imágenes para coaccionar, amenazar, acosar, cosificar o abusar". Una forma de IBA es el abuso sexual basado en imágenes (IBSA, por sus siglas en inglés),[29] que implica al menos uno de estos tres comportamientos: tomar, compartir o amenazar con compartir imágenes sexualmente explícitas sin consentimiento. Algunos estudiosos han defendido la inclusión de otras formas de abuso sexista y sexualizado, perpetrado mediante el uso de herramientas tecnológicas, como el *upskirting*, o la toma no consentida de una imagen por debajo de la falda o el vestido de una persona; falsificaciones realizadas por IA, o imágenes sexuales creadas no consentidas que muestran a la víctima de forma sexual, normalmente desarrolladas mediante herramientas de IA, y el *ciberflashing*, o envío no solicitado de imágenes de sus propios genitales a otra persona.[30] Otros ejemplos incluyen fotografiar o filmar a alguien sin su consentimiento o conocimiento,[31] o coaccionar a alguien para que adopte un comportamiento sexual no deseado en línea.[32]

Abuso sexual facilitado por la tecnología

4

El abuso sexual facilitado por la tecnología se refiere al uso de tecnologías de la comunicación, como teléfonos móviles, correo electrónico, redes sociales, salas de chat o sitios y aplicaciones de citas en línea, para cometer o facilitar agresiones o abusos sexuales.[33] En general, las experiencias sexuales no deseadas facilitadas por la tecnología implican tres comportamientos distintos: (1) la sextorsión, o coaccionar a alguien para que realice una actividad sexual mediante el chantaje, el soborno o las amenazas para que divulgue imágenes íntimas o información sensible; (2) el uso de la tecnología para contactar con una víctima potencial, por ejemplo a través de aplicaciones de citas, para luego perpetrar un delito sexual; y (3) el "abuso de poder", cuando los agresores solicitan y organizan que un tercero agreda sexualmente a una persona, a menudo utilizando una identidad falsa o haciéndose pasar por la víctima.[34] Además, el abuso sexual facilitado por la tecnología puede consistir en la "coerción del sexting" por la que los agresores obligan a alguien a enviar mensajes de texto con contenido sexual o a compartir imágenes y vídeos; y la "insinuación sexual no deseada", que consiste en recibir solicitudes no deseadas para hablar de sexo o hacer algo sexual.[35]

El reclutamiento de menores en línea es otro tipo específico de abuso sexual facilitado por la tecnología, en el que se contacta con niñas, niños y jóvenes a través de las redes sociales u otras plataformas digitales con el fin de agredirlos sexualmente. Se ha definido como un "proceso mediante el cual un agresor prepara a una niña/niño, a adultos y al entorno para el abuso. Esto incluye obtener acceso a la niña/niño, ganarse su complacencia y mantenerlo en secreto para evitar su revelación".[36]

Doxxing o doxeo

5

Doxxing es la divulgación no consentida de información personal. Implica la divulgación pública de información privada, personal y sensible de una persona, como la dirección de casa y de correo electrónico, números de teléfono, información de contacto del empleador y de los miembros de la familia, o fotos de sus hijos y de la escuela a la que asisten.[37] El doxxing es una forma de acoso en línea que rara vez se produce de forma aislada, sino que va acompañado de otras formas de acoso, como el IBA.[38] Las mujeres, especialmente de grupos minoritarios, tienen más probabilidades de ser objeto de doxxing, que afecta de manera desproporcionada a las mujeres racializadas y a las comunidades LGTBQI+.[39]

Según Douglas, hay tres tipos de doxxing: desanonimizar, o revelar la identidad de alguien; apuntar, o revelar información personal y privada de alguien que permita localizarlo físicamente, cuyas consecuencias pueden tener graves implicaciones para la seguridad de las mujeres; y deslegitimar, revelar información privada para socavar la credibilidad o reputación de alguien, avergonzarlo y humillarlo.[40] El doxxing a menudo conduce a más acoso físico y en línea, como recibir grandes cantidades de mensajes abusivos y amenazas por correo electrónico, teléfono o correo postal.[41]

Hackeo

El hackeo se define como el "uso de la tecnología para obtener acceso ilegal o no autorizado a sistemas o recursos con el fin de obtener información personal, alterar o modificar información, o calumniar y denigrar a la sobreviviente y/o a las organizaciones de violencia contra las mujeres".[42] El computador personal o el teléfono móvil de la sobreviviente pueden ser hackeados para obtener imágenes íntimas con el fin de perpetrar un IBA, chantajearla o coaccionarla para que realice una actividad sexual no deseada; o para obtener información privada que pueda ser utilizada para el doxxing u otros actos violentos.[43] Los agresores también pueden hackear el correo electrónico y las cuentas de redes sociales de una sobreviviente para controlar su actividad en línea, o incluso acceder a cuentas bancarias y controlar sus finanzas y/o perjudicarla económicamente.[44] Los hackers informáticos también pueden atacar los espacios en línea de organizaciones de derechos de las mujeres, activistas o figuras públicas debido a sus opiniones sobre el feminismo, la igualdad de género o los derechos sexuales, limitando así la participación de las mujeres en foros en línea y obstaculizando sus derechos.[45]

Reclutamiento y uso de la tecnología para localizar a sobrevivientes con el fin de perpetrar actos violentos.

La tecnología puede utilizarse para atraer a posibles víctimas/sobrevivientes a situaciones violentas[46] o para facilitar la agresión física o sexual en persona.[47] Los perpetradores y los traficantes pueden utilizar la tecnología para ponerse en contacto con posibles víctimas a través de publicaciones y anuncios fraudulentos en sitios y aplicaciones de citas, "agencias matrimoniales" o publicar falsas oportunidades de empleo y estudio.[48] Los perpetradores de la VPI también pueden utilizar determinadas tecnologías, como el espionaje o el seguimiento por GPS, para rastrear los movimientos y las actividades de las sobrevivientes, vigilarlas, controlarlas y localizarlas, con el fin de intimidarlas o agredirlas físicamente.[49] Esta forma de violencia también se manifiesta en la manera en que se induce a mujeres, jóvenes y niños a la trata de personas.[50] También se han conocido casos de jóvenes, niños, niñas y adolescentes, especialmente niñas, que han sido reclutados en Internet por el Estado Islámico de Irak y Siria (ISIS) a través de las redes sociales y atraídos por un matrimonio con la promesa de una vida utópica.[51]

Suplantación de identidad

La suplantación de identidad es el proceso de robar la identidad de alguien para amenazar o intimidar, así como para desacreditar o dañar la reputación de una persona.[52] Los agresores pueden apropiarse o crear cuentas en línea y sitios web falsos de mujeres para difundir información falsa y dañar su reputación,[53] arruinar sus relaciones personales y/o profesionales,[54] convocar a la violencia contra ellas a través de anuncios de trabajo sexual o aplicaciones de citas[55] o para obtener información sobre la sobreviviente.[56] La suplantación de identidad puede ser perpetrada por agresores individuales, pero también por agentes estatales. Por ejemplo, los agentes estatales tienen la capacidad de crear cuentas falsas en las redes sociales o suplantar la identidad de otras personas con el fin de perseguir a determinados grupos, como las personas LGBTQIA+.[57]

Discurso de odio

El discurso de odio es "cualquier tipo de comunicación verbal, escrita o de comportamiento que ataque o utilice un lenguaje peyorativo o discriminatorio con referencia a una persona o un grupo en función de lo que son, es decir, en función de su religión, etnia, nacionalidad, raza, color, ascendencia, género u otro factor de identidad".[58] El discurso de odio en línea por motivos de género y/o orientación sexual refuerza el sexismo sistémico al tiempo que deshumaniza y fomenta la violencia contra las mujeres y las niñas. En los últimos años, el discurso de odio contra las mujeres, las niñas y las personas LGTBQI+ ha aumentado considerablemente, y las plataformas de las redes sociales y los foros de chat en línea acogen a grupos que promueven el odio y la violencia contra las mujeres[59].

Difamación

10

La difamación consiste en la difusión pública de información falsa que daña la reputación de una persona y que tiene la intención de humillar, amenazar, intimidar o castigar a la víctima[60]. Dadas las estrictas normas de género que rigen la sexualidad femenina, las declaraciones difamatorias sobre la sexualidad de las mujeres son especialmente perjudiciales para la reputación de las personas sobrevivientes. De hecho, la mayoría de los ataques difamatorios en línea contra mujeres y niñas suelen centrarse en su sexualidad.[61]

Limitar o controlar el uso de la tecnología

11

Especialmente en las relaciones íntimas abusivas, los agresores pueden utilizar la tecnología para ejercer abuso y control sobre la sobreviviente, rastreando, vigilando o restringiendo sus movimientos, comunicaciones y actividades. Estos comportamientos abusivos incluyen obligar a la víctima a dar sus contraseñas, obtener acceso no autorizado a sus cuentas en línea, limitar su uso de dispositivos tecnológicos controlando digital o físicamente el acceso a dispositivos o cuentas e inspeccionar los dispositivos de la víctima.

Las parejas íntimas y los familiares tienen mayor acceso a los dispositivos y a la información personal de una persona y pueden ejercer un poder coercitivo y de control sobre ella. Por ejemplo, las parejas íntimas pueden conocer y monitorear las cuentas bancarias y las redes sociales del otro, y compartir contraseñas y dispositivos, voluntaria o involuntariamente. En las relaciones íntimas abusivas, las amenazas a la intimidad de la pareja por el uso de la tecnología pueden ser precursoras de otras formas de abuso.[62]

Prevalencia de la VBG-FT

Cada vez se dispone de más estudios que ponen de relieve la prevalencia de las formas de VBG-FT. Sin embargo, estas investigaciones utilizan diferentes metodologías y herramientas de encuesta, así como diferentes grupos de población y miden formas específicas de VBG-FT.

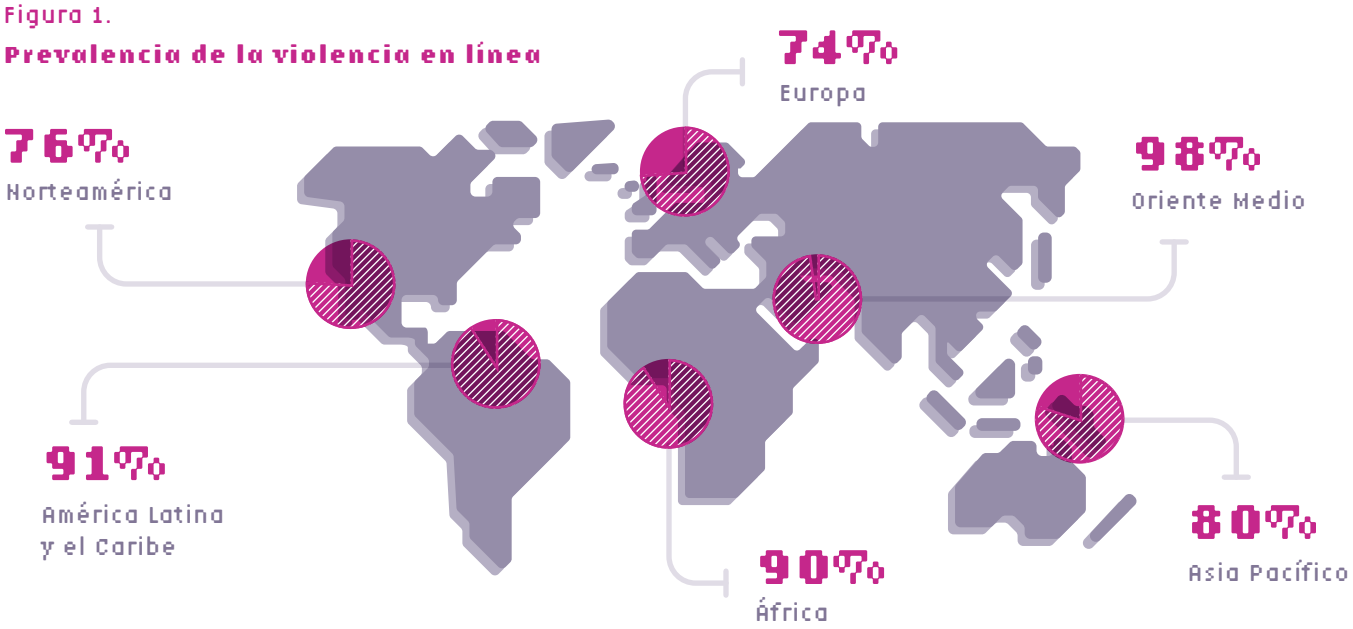
Medir el alcance y el impacto de los actos violentos cometidos en línea y/o a través de medios digitales y tecnológicos es una tarea de enormes proporciones, por varias razones:

- Ausencia de una definición normalizada de la VBG-FT y de sus diversas formas;
- La prevalencia puede medirse de una forma que no tiene en cuenta el nivel de accesibilidad a la tecnología y a los espacios digitales de las mujeres y las niñas;
- Van surgiendo nuevas formas de VBG-FT a medida que aparecen nuevas tecnologías, las antiguas se utilizan de forma diferente y se dispone de nuevos espacios digitales y en línea.

En conjunto, esto significa que no existe una única medida cuantitativa validada en la cual basarse para obtener datos de prevalencia a escala local, nacional, regional y mundial[63] que respalden las políticas basadas en la evidencia, las intervenciones de los programas (respuesta y prevención) y las medidas de rendición de cuentas.

Un reciente estudio realizado por Economist Intelligence Unit en 2021 con mujeres de los 51 países con tasas más altas de penetración de Internet[64] ha demostrado que, a nivel mundial, el 38% de las mujeres con acceso a Internet han sufrido violencia en línea, el 63% de las mujeres conocen a alguien que ha sido víctima de ella y el 85% de las mujeres han sido testigos de la violencia en línea perpetrada contra otra mujer[65]. Este estudio también ofrece estimaciones regionales de la prevalencia de la violencia en línea contra las mujeres, como se representa en la Figura 1.

Figura 1.
Prevalencia de la violencia en línea



Nuestro estudio abarca los 51 primeros países por número de personas conectadas a Internet. Fuente: https://onlineviolencewomen.eiu.com/

Es probable que estos resultados subestimen la prevalencia real de la VBG-FT, dado que este estudio sólo tuvo en cuenta la violencia en línea y no incluyó otras formas de violencia facilitada por la tecnología perpetradas a través de teléfonos móviles, GPS y otras tecnologías. Además, sólo incluía a mujeres y no a adolescentes, que probablemente corren un mayor riesgo de sufrir VBG-FT. De hecho, un estudio realizado por Plan International entre mujeres jóvenes y adolescentes (entre 15 y 25 años) de 31 países de todo el mundo puso de manifiesto que las generaciones más jóvenes utilizan más y con mayor frecuencia las redes sociales, lo que aumenta su exposición a la VBG-FT. El informe reveló que el 58% de las mujeres y niñas entre 15 y 25 años habían sufrido acoso en línea[66].

Aunque no es exhaustiva, se ha llevado a cabo una amplia revisión de las encuestas, contenidas en el Apartado 3. Aunque el corpus de investigación es pequeño, los estudios generalmente no miden la VBG-FT en su forma más inclusiva, sino que examinan y miden formas específicas de VBG-FT. Además, los datos se limitan a estudios localizados con muestras relativamente pequeñas.

La naturaleza omnipresente de la VBG-FT es un importante motivo de preocupación. Los datos indican unas estimaciones de prevalencia del abuso en línea de hasta el 58%[67], lo que supera con creces las estimaciones mundiales actuales de la experiencia vital de la VPI y la violencia sexual fuera de la pareja, que es del 31% de las mujeres de entre 15 y 49 años[68].

Esto sugiere que allí donde los índices de conectividad de Internet son elevados y las mujeres y niñas acceden a la tecnología, los índices de VBG-FT casi duplican los índices de VPI. A medida que aumenten la tasa de penetración de Internet y el acceso a las tecnologías, estas tendencias irán en aumento.

Además de la prevalencia de la VBG-FT, se han recolectado algunos datos sobre las actitudes ante el impacto del acoso en línea. Los resultados de los Estados Unidos han mostrado una diferencia de género en las actitudes, donde la mitad de las mujeres afirman que el contenido ofensivo en línea se excusa con demasiada frecuencia como no significativo, mientras que el 64% de los hombres, y el 73% de los hombres jóvenes, afirman que el contenido ofensivo en línea se toma demasiado en serio.[69] Aunque de alcance limitado, esta investigación, al igual que los datos de prevalencia disponibles, crea motivos de preocupación que requieren que se lleven a cabo encuestas similares sobre las actitudes a una escala más amplia.

Los datos de prevalencia disponibles, combinados con una comprensión limitada de las repercusiones de la VBG-FT y la falta de mecanismos de rendición de cuentas y de respuestas coordinadas, ofrecen una imagen sombría del estado actual de este fenómeno y la respuesta a la VBG-FT. Es fundamental que se acuerden definiciones estandarizadas y metodologías de recopilación de datos relacionados con la VBG-FT para proporcionar una sólida base empírica de cara al futuro.

58%

31%

Los datos indican estimaciones de prevalencia del abuso en línea de hasta el 58%, lo que supera con creces las estimaciones mundiales actuales de la experiencia vital de la VPI y la violencia sexual fuera de la pareja que es el 31% de las mujeres de 15 a 49 años.

¿Quién sufre VBG-FT?

Aunque las mujeres y las niñas son las más expuestas al riesgo de sufrir VBG-FT, hay grupos específicos de mujeres y niñas a los que se ataca de forma desproporcionada. Entre ellos se encuentran las mujeres con discapacidad, las adolescentes, las mujeres racializadas, las mujeres en espacios públicos, como las periodistas o las políticas, y las personas LGBTQIA+.[70]

Niñas y Adolescentes

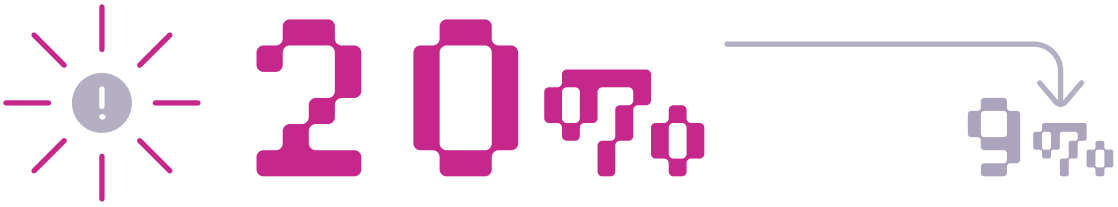
La tecnología se está convirtiendo cada vez más en una parte central de la vida de los adolescentes. Los adolescentes de ambos sexos utilizan la tecnología y las plataformas en línea para aprender y obtener información y para mantenerse en contacto con sus compañeros.[71] Un estudio realizado por Plan International con 14.000 niñas de 31 países de todas las regiones reveló que el uso de las redes sociales es más frecuente a una edad temprana (15 años),[72] aunque otras fuentes revelan que los niños y las niñas se conectan a edades mucho más tempranas.[73]

Las adolescentes son un grupo cada vez más vulnerable a la VBG-FT debido a su creciente participación y uso de las tecnologías y los espacios digitales[74]. Por ejemplo, el 80% de las imágenes de casos de materiales de abuso sexual infantil son de niñas de entre 11 y 13 años[75], las adolescentes suelen ser objeto de abuso sexual digital en el contexto de la violencia de pareja.[76] El 58% de las mujeres jóvenes y adolescentes han sido acosadas en línea, según el estudio de Plan International, y el 85% de ellas sufrieron varios tipos de VBG-FT incluido el lenguaje abusivo e insultante (59%), body shaming (39%), las amenazas de violencia sexual (39%) y física (21%), el acoso sexual (37%) o el acoso (32%).[77] Otro estudio realizado por la World Wide Web Foundation y la Asociación Mundial de las Guías Scouts reveló que el 52% de las jóvenes y las niñas han sufrido abusos en línea y que el 68% de estos han tenido lugar en plataformas de redes sociales.[78] Aunque el acoso suele comenzar entre los 14 y los 16 años, algunas niñas declararon su primera experiencia de VBG-FT a los 8 años. La VBG-FT contra las adolescentes también es interseccional y muchas de las que han sido acosadas y que se identifican como minoría étnica, LGBTQIA+ o con una discapacidad dijeron que fueron acosadas por ello.[79] Además, el uso de plataformas de redes sociales puede tener un impacto negativo importante en la salud mental de los jóvenes, en particular de las adolescentes.[80]

Mujeres en la vida pública y profesional

Las mujeres son un objetivo desproporcionado de la VBG-FT cuando su vida profesional se apoya en una presencia en línea. Las defensoras de los derechos humanos, las activistas, las periodistas, las blogueras, las artistas y las políticas, por ejemplo, son grupos de profesionales y líderes que se ven desproporcionadamente afectadas por la VBG-FT[81]. Estos grupos de mujeres utilizan plataformas digitales y redes sociales para apoyar su vida profesional como parte de su compromiso con el público en general. Las mismas plataformas en las que se basan para aumentar el nivel de divulgación pública para la incidencia también están siendo utilizadas por los perpetradores para amenazar, acosar, acechar y promover discursos de odio.[82] Una encuesta reciente realizada por la UNESCO, en la que participaron 901 periodistas de 125 países, reveló que el 73% de las mujeres periodistas habían sido objeto de violencia en línea, y el 20% de las mujeres periodistas fueron atacadas fuera de línea como consecuencia directa de dicha violencia en línea.[83] Del mismo modo, un estudio mundial realizado por la Unión Interparlamentaria muestra que el 41,8% de las mujeres que ejercen la política habían visto imágenes o comentarios con connotaciones sexuales, difamatorias o humillantes de sí mismas difundidos a través de las redes sociales, y el 44,4% habían recibido amenazas de "muerte, violación, palizas o secuestro durante su mandato parlamentario"[84].

Las mujeres que utilizan las plataformas digitales para el activismo y la incidencia de sus intereses son también un blanco particular y desproporcionado. Nada menos que el 88% de las mujeres que respondieron a una encuesta realizada en el Reino Unido, que utilizan las redes sociales habitualmente para expresar sus ideas feministas, han sido objeto de VBG-FT en Twitter, (el 60% en Facebook y el 46% en blogs) en forma de troleo, difamación, acoso y amenazas de violencia física y sexual[85]. Además, la edad es un factor de protección en la comisión de VBG-FT. Como detalló Plan International, las mujeres jóvenes y las adolescentes que hablan en línea sobre cuestiones políticas, feminismo, raza o salud y derechos sexuales y reproductivos se enfrentan a una considerable reacción violenta. De hecho, el 47% de quienes respondieron a la encuesta de Plan International afirmaron haber sido atacadas por sus opiniones.[86]

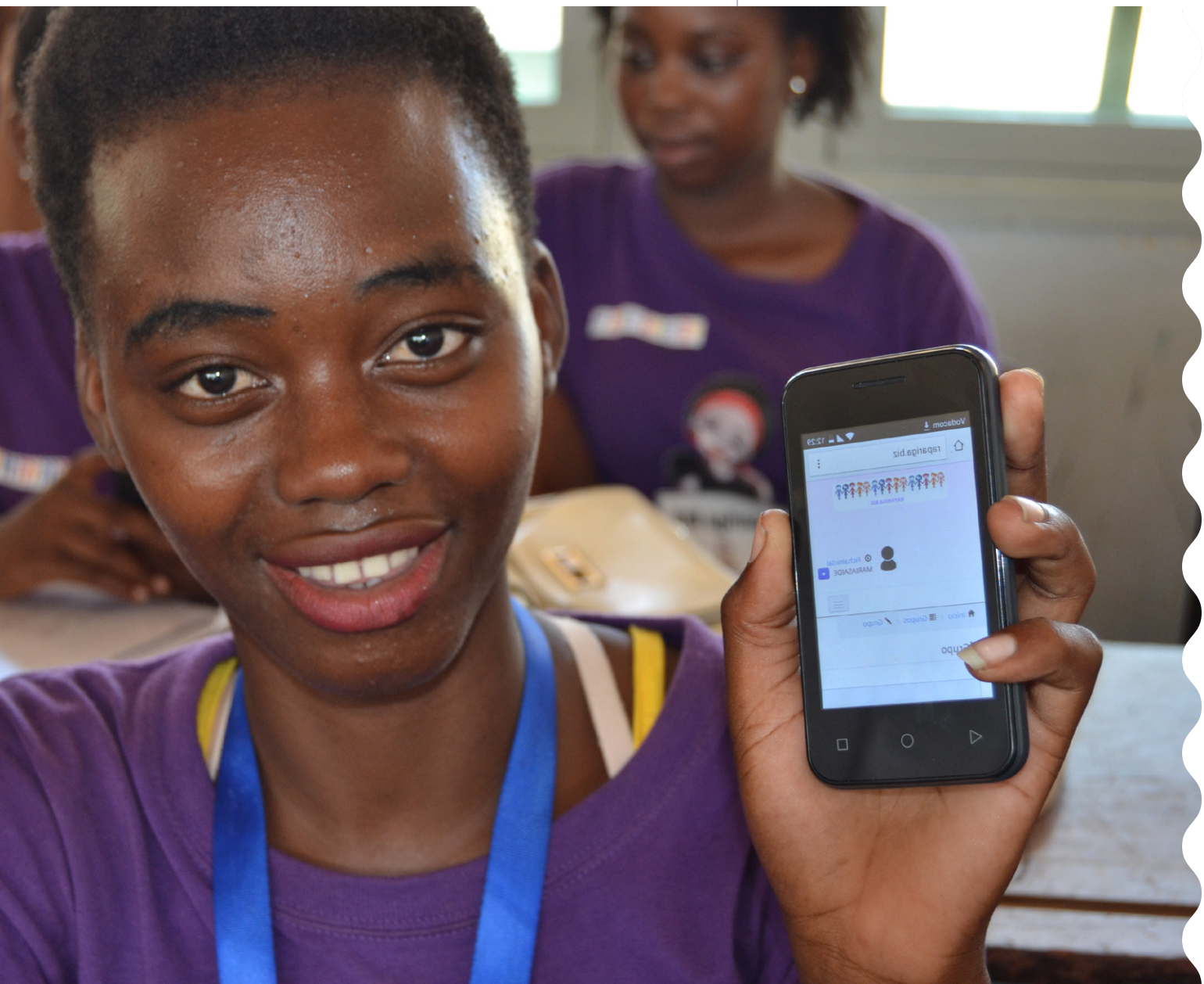


El 20% de las personas LGBTQIA+ de la diversidad étnica-racial fueron objeto de VBG-FT, frente al 9% de las personas LGBTQIA+ que no pertenecen a estos grupos etnico-raciales.

Importancia de la interseccionalidad

La VBG-FT va más allá de la misoginia y el sexismo, y también tiene sus raíces en la homofobia, la transfobia, el racismo, el capacitismo y otras formas de discriminación. Las mujeres y las personas con factores de identidad que se entrecruzan son atacadas y discriminadas en mayor medida y de formas distintas que combinan un lenguaje sexista, racista y homófobo.[87] Las mujeres afrodescendientes, las mujeres indígenas, las mujeres de minorías religiosas, las mujeres LGBTQA+ y las personas no binarias, así como las mujeres con discapacidades, son objeto de agresiones únicas y contundentes.[88] Las mujeres jóvenes y las adolescentes racializadas, con discapacidades y que se identifican como LGBTQA+ se ven afectadas de forma desproporcionada por este tipo de abusos.[89]

Las investigaciones demuestran que las personas LGBTQIA+ tienen más probabilidades de ser objeto de diferentes formas de VBG-FT, como la agresión sexual, el acoso y el discurso de odio[90]. Por ejemplo, un estudio con 332 activistas LGBTQ+ y de diversidad sexual de todo el mundo reveló que todos los encuestados trans e intersexuales habían recibido amenazas y comentarios intimidatorios en línea, y que los encuestados LGBTQIA+ sufren tasas más altas de VBG-FT que sus homólogos heterosexuales.[91] Además, las mujeres y niñas negras, asiáticas, pertenecientes a poblaciones étnico-raciales sufren más ataques que las mujeres y niñas blancas. Un estudio realizado en el Reino Unido con 5.000 personas LGBTQIA+ reveló que el 20% de las personas LGBTQIA+ de diversidad étnica-racial sufrían VBG-FT, frente al 9% de las personas LGBTQIA+ blancas[92].



La vida digital es la vida real: El impacto de la VBG-FT

A pesar de que a menudo se percibe como una forma de VBG menos grave y dañina, la VBG-FT puede tener consecuencias tan graves para la salud y la vida de las mujeres y las niñas como la violencia física y sexual. La naturaleza *pública, omnipresente, repetitiva* y *perpetua* de la VBG-FT, así como la continua violencia en línea y fuera de línea, provocan un miedo y una inseguridad constantes que se ven agravados por la falta de servicios de respuesta especializados y accesibles y la percepción errónea predominante de que la VBG-FT no es "real".

La naturaleza múltiple y repetitiva de la VBG-FT significa que la mayoría de las mujeres experimentan múltiples tipos de abuso y muchas lo experimentan como una parte rutinaria de sus vidas en línea, ya sea porque tienen una presencia en línea con fines profesionales o son activistas y defensoras de los derechos humanos. Es probable que la VBG-FT se experimente como un patrón y un curso de conducta más que como un conjunto de actos individuales. Esto también tiene el efecto de que las respuestas legales, que a menudo tratan cada comunicación como un delito independiente, se quedan cortas a la hora de abordar la acumulación de daños a largo plazo.[93]

La VBG-FT a menudo tiene lugar en un continuo en el que las acciones que comienzan en el espacio digital pueden llevar a la perpetración de VBG fuera de línea y viceversa.[94] Por ejemplo, la VBG-FT a menudo se comete en el contexto de relaciones abusivas en las que la tecnología y los espacios digitales proporcionan una vía para la continuación de la violencia a pesar de no tener proximidad física con la sobreviviente.

Un estudio realizado entre estudiantes universitarias de EE. UU. ha demostrado que el 92,6% de las víctimas de VPI también sufrieron agresiones facilitadas por la tecnología, lo que demuestra la continuidad de la violencia en los espacios físicos y no físicos[95]. En otros casos, los compañeros íntimos pueden utilizar las tecnologías de la información y la comunicación para acosar, vigilar, rastrear y vigilar a las mujeres, en combinación con el acoso en persona.[96] Por ejemplo, en el Reino Unido, un pequeño estudio realizado entre 307 sobrevivientes de VPI reveló que el 45% de ellas había sufrido abusos a través de la tecnología durante la relación, y el 48% experimentó VBG-FT después de que ésta terminara.[97]

A la inversa, el acoso y las amenazas en línea exacerban, desencadenan e impulsan las agresiones físicas y sexuales fuera de línea.[98] Por ejemplo, una encuesta realizada en Malawi reveló que el 53,7% de las mujeres sufrían abusos físicos exacerbados por la violencia en línea y que el 34,3% sufrían daños físicos o lesiones como consecuencia de ello.[99] En otros casos, las formas sexualizadas de VBG-FT, como la violencia sexual contra las mujeres, han conducido a la violencia contra las mujeres por motivos de honor.[100]

Las sobrevivientes de la VBG-FT suelen manifestar graves trastornos emocionales y psicológicos, ansiedad, depresión, trastorno de estrés postraumático y, en casos extremos, ideación suicida, autolesiones o intentos de suicidio.[101] Amnistía Internacional realizó un estudio en ocho países de ingresos altos y encontró que el 54% de las mujeres que habían sido objeto de VBG-FT sufrían ataques de pánico, ansiedad o estrés.[102] Del mismo modo, un estudio realizado con 326 mujeres en el sur de la India reveló que el 28% de las mujeres encuestadas se sentían ansiosas o deprimidas y que el 6% había intentado autolesionarse de alguna forma.[103] Según un estudio reciente realizado por Plan International en 31 países, el 42% de las mujeres jóvenes y las niñas declararon sufrir estrés mental o emocional y una menor autoestima o pérdida de confianza en sí mismas.[104] Concretamente, las personas sobrevivientes de abuso sexual basado en la imagen (IBSA) pueden sufrir trastornos de salud mental y angustia psicológica en comparación con las personas sobrevivientes de agresiones sexuales.[105]

Las mujeres y niñas que han sido víctimas de formas sexuales de VBG-FT, en concreto de IBA, describen la experiencia como algo que tiene un impacto devastador en sus vidas. Afirman que sus relaciones se deterioran, que tienen sentimientos constantes de aislamiento, miedo, desconfianza e inseguridad. Estas experiencias se describen como similares en naturaleza e impacto a las que sienten las personas sobrevivientes de la violencia sexual.[106]

La VBG-FT también contribuye a aumentar el aislamiento en línea y fuera de línea en un momento en que las redes de apoyo son cruciales. Es decir, las mujeres que han sido víctimas o testigos[107] de VBG-FT disminuyen su participación en línea y su compromiso con la tecnología, y restringen o autocensuran sus actividades en las plataformas en línea. Si bien esto es particularmente preocupante en el contexto de las mujeres que dependen de su presencia en línea como parte de su vida profesional, incluidas las periodistas y las políticas, esta violencia sirve para silenciar efectivamente a todas las mujeres. Las ramificaciones de esta situación no pueden subestimarse.

Esto, unido a los efectos psicológicos y mentales de la VBG-FT, tiene importantes consecuencias para la participación política y social de las mujeres, las oportunidades de empleo y el acceso a la educación y la información.[108] Por ejemplo, en todo el mundo, el 18% de las mujeres jóvenes y las niñas que fueron objeto de VBG-FT experimentaron posteriormente problemas en la escuela.[109] En Malawi, el 6% de las víctimas perdieron oportunidades de educación debido a la VBG-FT.

92,6%

El 92,6% de las que sufrieron VPI también sufrieron agresiones facilitadas por la tecnología, lo que demuestra la continuidad de la violencia en los espacios físicos y no físicos.

Las mujeres que han sido víctimas de la VBG-FT, especialmente de las formas sexuales de la VBG-FT, a menudo son estigmatizadas y su reputación se ve dañada. Al igual que ocurre con otras formas de VBG, a menudo se culpa a las mujeres de la violencia que sufren y se desestima la violencia por no ser "real". De hecho, se han documentado casos de sobrevivientes que han sido despedidas o expulsadas de la escuela después de que sus imágenes íntimas se distribuyeran sin su consentimiento.[110] Las mujeres también pueden ser atacadas directamente con el único propósito de dañar su reputación para asegurarse la pérdida del empleo. El daño a la reputación debido a la VBG-FT puede acarrear importantes pérdidas económicas para las mujeres propietarias de un negocio, especialmente en las zonas rurales.[111] En Malawi, el 76,1% de las mujeres que fueron objeto de VBG-FT sufrieron algún tipo de pérdida de ingresos, y el 12% no pudieron conseguir un nuevo empleo.[112] A escala mundial, el 7% de las mujeres jóvenes y niñas que fueron objeto de VBG-FT tuvieron problemas para encontrar o mantener un empleo.[113]

Además, la VBG-FT tiene un impacto importante en la productividad de las mujeres. De hecho, el 55% de las participantes en un estudio realizado en ocho países de renta alta declararon que la VBG-FT disminuía su capacidad para concentrarse en las tareas cotidianas. Este mismo estudio sugirió que, cuando las mujeres se autocensuran después de haber sufrido VBG-FT, pueden perder contactos y oportunidades de empleo.[114] Sin embargo, los daños económicos de la VBG-FT no se detienen ahí, ya que las sobrevivientes a menudo tienen que asumir altos costos por honorarios legales, atención médica, reubicación o eliminación de su información o imágenes en línea.[115] También pueden experimentar daños económicos debido al abuso con fines financieros, o a la pérdida de su hogar y propiedades.[116]

La VBG-FT es también un obstáculo importante para la participación igualitaria de las mujeres en la vida pública, silenciando las voces de las mujeres y limitando su derecho democrático a la representación y la participación. Las mujeres son objeto de ataques por las opiniones, contribuciones y contenidos que crean a través de su presencia en Internet. Las mujeres políticas, activistas y periodistas no son el único objetivo de los perpetradores de VBG-FT, sino que el 47% de las mujeres jóvenes que se manifestaron políticamente también sufrieron ataques por sus opiniones[117]. Los ataques sexistas contra las mujeres en la vida pública no sólo están dirigidos a sus opiniones, sino que tienden a ser de naturaleza sexual, haciendo referencia a su aspecto físico y la vida personal de las mujeres[118]. Este silenciamiento de las mujeres en el espacio digital es un ataque contra su libertad de expresión y tiene importantes repercusiones en la presencia de las mujeres en los foros de debate y en los espacios de toma de decisiones, así como en su disposición a asumir funciones de liderazgo, lo que refuerza aún más los roles y las estructuras patriarcales[119].

Los efectos de la VBG-FT no son sólo personales. También hay importantes repercusiones sistémicas y estructurales. La menor participación de las mujeres en el espacio digital no sólo amplía la brecha digital de género, sino que también refuerza la desigualdad de género, las estructuras de poder patriarcales y las normas de género.[120] Dada la creciente prevalencia y el uso de los espacios y tecnologías en línea y digitales para acceder a los servicios, el empleo y la educación, se constituye como un obstáculo para que las mujeres, en toda su diversidad, accedan a sus derechos humanos. Como tal, la prevalencia de la VBG-FT ya representa una crisis, siendo un obstáculo significativo para el desarrollo sostenible y el avance hacia la igualdad de género.[121]

Perfil de los perpetradores de la VBG-FT

La VBG-FT puede ser una herramienta de la VPI o por motivos de pareja, pero también puede ser perpetrada por conocidos, compañeros de trabajo y desconocidos, incluidas personas u organizaciones (por ejemplo, por motivos políticos o ideológicos) con la permisividad, y a veces complicidad, de las plataformas de redes sociales y las empresas tecnológicas[122].

La tecnología también ha brindado oportunidades para que se cometan actos de violencia anónimos y en grupo con relativa impunidad.

La asequibilidad y accesibilidad de la tecnología para los agresores está llevando a la VPI a nuevos espacios. Los datos disponibles sugieren que la mayor parte de la VBG-FT es perpetrada por parejas íntimas actuales o anteriores. Por ejemplo, un estudio australiano realizado con proveedores de servicios de VBG reveló que los perpetradores más comunes de este tipo de violencia eran las exparejas íntimas, las parejas íntimas actuales, y las relaciones sexuales de corta duración o casuales[123].

Parejas o exparejas íntimas

En el contexto de la VBG-FT, la VPI se utiliza a menudo para intimidar, coaccionar y mantener el control sobre las personas sobrevivientes con el fin de mantener una relación o como castigo o venganza por haberlas abandonado, así como una plataforma para incitar a otros a hacerles daño o interferir en los procedimientos legales, entre otras razones[124]. Las parejas íntimas abusivas acosan, monitorean y amenazan a las sobrevivientes por medio de servicios de localización, redes sociales y programas espía que se encuentran fácilmente disponibles en las tiendas de aplicaciones oficiales, algunos de los cuales se anuncian a los abusadores como herramientas para "atrapar infieles".[125] Las parejas íntimas abusivas pueden restringir o impedir el acceso de las sobrevivientes a sus teléfonos móviles y dispositivos tecnológicos, limitando su capacidad para comunicarse con otras personas y buscar ayuda. Los agresores suelen tener acceso a las cuentas y los círculos sociales de la sobreviviente, lo que les facilita el acceso ilícito a sus dispositivos y cuentas, incluidas las de correo electrónico y redes sociales, e información bancaria. Tener acceso a estos datos privados puede permitir a los perpetradores instalar programas espía, rastrear y monitorear la ubicación y el uso de la tecnología, robar o borrar información e intimidar a las personas sobrevivientes.

También pueden amenazar y chantajear a la superviviente para que revele fotos íntimas o información privada, y acosar a la sobreviviente y a sus círculos sociales a través de diferentes medios digitales.[126]

Las parejas íntimas a menudo son capaces de continuar con el abuso incluso después de que la relación termina.[127] De hecho, en un pequeño estudio realizado en el Reino Unido con 307 mujeres que habían sido víctimas de VIP, el 45% de ellas también habían sido víctimas de VBG-FT durante la relación y el 48% después de terminada [128].

Agentes estatales

El Estado también puede ser perpetrador de VBG-FT. Los agentes estatales tienen la posibilidad de acceder a grandes cantidades de información detallada sobre las víctimas, incluidos los datos de salud en línea, por ejemplo, que contienen información muy delicada y confidencial porque los datos se recopilan habitualmente en los historiales médicos y los sistemas de gestión de la información. Los agentes estatales también suelen tener una gran capacidad para vigilar, acosar, rastrear y obtener datos sobre las personas con el fin de ejercer la violencia, cuyas consecuencias pueden tener implicaciones de género. Los agentes estatales pueden utilizar la tecnología y los datos para perpetrar actos de violencia contra, por ejemplo, activistas, abogadas, periodistas, personas que no se ajustan a las normas de género, minorías sexuales o dirigentes políticos de oposición.[129] Además, los gobiernos tienen la capacidad de bloquear el acceso a la información y a los sistemas de gestión de la información y servicios de salud sexual y reproductiva, como el aborto en línea y la anticoncepción de emergencia.

Aunque los Sistemas de Gestión de la Información sobre VBG[130] aplican las normas más estrictas posibles de recopilación y almacenamiento de datos sólidos y éticos para garantizar la confidencialidad de la información de las personas sobrevivientes, la ciberseguridad y el uso indebido de la tecnología y la información por parte del Estado y otros actores, incluidas las partes no estatales en un conflicto, siguen siendo un riesgo. Muchos países tienen "una capacidad inadecuada para implementar eficazmente sistemas de información seguros; marcos jurídicos débiles o inexistentes para la protección de datos; y carecen de una unidad específica en los ministerios de salud, con personal debidamente cualificado, para supervisar éticamente los datos".[131]

Extraños y trolls

A medida que la sociedad se vuelve cada vez más digital, surgen nuevas formas de socializar y relacionarse con nuevas personas y desconocidos. Las formas tradicionales de acoso en los espacios públicos físicos se han trasladado a la esfera en línea, lo que permite a los agresores identificar y atacar fácilmente a mujeres y niñas en plataformas de redes sociales, sitios web y aplicaciones, manteniendo el anonimato[132].

Los trolls suelen ser desconocidos que publican deliberadamente comentarios o mensajes, suben imágenes o vídeos y crean hashtags con el fin de molestar, provocar o incitar a la violencia contra las mujeres y las niñas para su propia diversión[133]. Los desconocidos y los trolls han sido perpetradores de VBG-FT desde los inicios de Internet: se han denunciado comentarios misóginos y sexistas, amenazas de violación e información difamatoria desde principios de la década de 2000 (por ejemplo, Auto Admit), con casos recientes de mayor radicalización y campañas organizadas de acoso contra las mujeres (por ejemplo, GamerGate).

Un estudio realizado por Plan International en 31 países de todas las regiones reveló que los desconocidos son los perpetradores más comunes de VBG-FT contra las mujeres jóvenes y las niñas (36%), seguidos por los usuarios anónimos de las redes sociales (32%) y los conocidos en las redes sociales (29%). Cabe destacar que el 16% de los abusos en línea contra mujeres jóvenes y niñas son perpetrados por grupos de desconocidos[134].

Según los informes, el acoso por parte de desconocidos es más aterrador y difícil de detener, y tiende a provenir de hombres, que se enfurecen especialmente cuando las mujeres y las niñas expresan sus opiniones y no se ajustan a las normas e ideas tradicionales de feminidad.[135] Entre las mujeres mayores, el 59% de las que sufrieron abusos o acoso en Twitter dijeron que habían sido atacadas por desconocidos.[136]

Rendición de cuentos

La rendición de cuentas a las personas sobrevivientes de la VBG-FT es quizás uno de los ámbitos más difíciles de abordar. No solo las tecnologías y los espacios digitales cambian constantemente, sino que los perpetradores pueden ser anónimos y resulta difícil legislar en todas las jurisdicciones.

Responsabilidad del Estado

Los Estados tienen la responsabilidad de desarrollar marcos legislativos, políticos y normativos para abordar la VBG-FT con el fin de garantizar la rendición de cuentas de los perpetradores, pero también para garantizar la seguridad de las plataformas en línea, los espacios digitales y el uso de la tecnología. Sin embargo, los marcos jurídicos y las políticas actuales rara vez tienen en cuenta la VBG-FT dentro de las leyes y políticas existentes que abordan la VBG y, aunque algunos países pueden tener leyes y políticas para la salvaguarda y la seguridad en línea, a menudo son genéricas o insensibles o neutrales en cuanto al género, y no toman las medidas adecuadas para detener el daño digital.[137] Estos marcos son a menudo insuficientes y no se mantienen al día con las nuevas tecnologías, plataformas en línea y otros medios a través de los cuales se perpetúan y amplifican nuevas formas de VBG. Según la Economist Intelligence Unit, "en 64 de 86 países, las agencias encargadas de hacer cumplir la ley y los tribunales parecen no tomar las medidas correctivas adecuadas para hacer frente a la violencia contra las mujeres en línea".[138] Estos datos ponen de relieve una importante brecha estructural que deja los mecanismos de rendición de cuentas a la buena voluntad de las empresas privadas de tecnología.

Algunas formas de VBG-FT están legisladas y a menudo tipificadas como delito, en particular las que responden a definiciones de delitos penales preexistentes o a causas de acción civil. Por ejemplo, algunas formas de abuso sexual basado en la imagen (IBSA), actos de suplantación de identidad, difamación, amenazas de violencia, acoso y otras formas de invasión de la privacidad se configuran como delitos civiles y/o criminales el algunos países[139].

Sin embargo, otras formas de VBG-FT, como el acoso en línea no delictivo, el trolling, el *mobbing* en línea o la creación y difusión de falsificaciones realizadas por IA no sexualizados, pueden considerarse tan solo "un discurso o una mera expresión".[140]

Además, cuando existen políticas y leyes, su implementación no es uniforme. Entre las causas de esta implementación limitada se encuentran la percepción entre los oficiales encargados de hacer cumplir la ley de que la VBG-FT no es un delito grave, así como los prejuicios y las ideas erróneas internas en materia de género, el sexismo y las dinámicas de poder dentro de los sistemas patriarcales de la ley y de justicia, lo que refuerza la culpabilización de la víctima. Además, las interpretaciones de la VBG-FT pueden no cumplir los elementos de las definiciones de delitos penales existentes de violencia contra las mujeres o de VBG en la ley. Además, la capacidad de las agencias encargadas de hacer cumplir la ley y de los sistemas judiciales para acusar y condenar adecuadamente a los delincuentes cuando no se puede rastrear la identidad del delincuente o delincuentes significa que la conducta en línea se comete con impunidad. Por último, cuando el delito se comete en una jurisdicción distinta a la de la persona sobreviviente, los medios para acceder a la rendición de cuentas se vuelven aún más improbables.


love question life answer

Alemania ha puesto en marcha la "Ley para Mejorar la Aplicación de la Ley en las Redes Sociales", o Netzwerkdurchsetzungsgesetz (NetzDG). Esta ley obliga a las plataformas de redes sociales como Twitter, Reddit y Facebook a eliminar el discurso de odio y otros contenidos ofensivos en un plazo de 24 horas. No retirar los contenidos prohibidos puede acarrear multas de hasta 50 millones de euros. Por ello, las plataformas de redes sociales están cumpliendo la ley, por ejemplo, creando centros de eliminación para monitorear los contenidos y aplicando en mayor medida sus propias normas comunitarias. En 2020, la ley se modificó para exigir una mayor rendición de cuentas a las empresas de redes sociales, que ahora están obligadas a informar de los contenidos nocivos a la German Federal Criminal Police Office para permitir el enjuiciamiento penal.[141] Dicho esto, el éxito de la NetzDG en la reducción del discurso de odio y los contenidos nocivos y violentos es difícil de monitorear y evaluar.142

En la Unión Europea, la propuesta de la Ley de Servicios Digitales (2020) reconoce explícitamente los daños sistémicos que pueden causar las plataformas digitales e impone mayores obligaciones a las grandes plataformas en línea, para que evalúen periódicamente y respondan a los riesgos derivados del uso de sus servicios[143].

En Australia, la regulación de la seguridad en línea ha sido, y sigue siendo, una prioridad permanente para los reguladores. De hecho, la Ley de Seguridad en Línea de 2021 (Cth) (la "Ley"), que se aprobó recientemente en julio de 2021, exigirá que los proveedores de servicios en línea, los proveedores de servicios de redes sociales y otros proveedores de servicios de Internet designados tengan los siguientes seis meses para garantizar que sus políticas y procedimientos están actualizados y cumplen la legislación australiana. Las empresas incluidas en la Ley deben proteger de forma proactiva a los usuarios australianos y tener capacidad para responder a los avisos de la Comisión con poca antelación para retirar el material perjudicial. En efecto, se impone claramente a las empresas la obligación de mantener espacios seguros. La Ley también sigue apoyando al organismo oficial independiente, la eSafety Commission (la "Comisión"), cuyas principales funciones son hacer cumplir la Ley y administrar un sistema de denuncias:

- material de ciberbullying dirigido a un niño australiano;
- intercambio no consentido de imágenes íntimas;
- material de ciberabuso dirigido a un adulto australiano; y
- un plan de contenidos en línea.

Es de vital importancia que la carga de la retirada del material nocivo pase de la persona sobreviviente al organismo regulador para gestionar la retirada inmediata del material infractor directamente con la empresa infractora. Además, la Comisión colabora estrechamente con las empresas privadas en la incorporación de elementos de seguridad en el diseño de las plataformas, creando asociaciones para abordar la VBG-FT.[144]

Empresas privadas de tecnología

Las empresas tecnológicas privadas engloban una amplia gama de organizaciones, entre las que se incluyen las siguientes:[145]

- Proveedores de servicios de Internet designados - entidades que permiten a los usuarios finales acceder a materiales en línea, y proveedores de servicios de Internet, que son las entidades que prestan servicios de transporte por Internet, incluidos, entre otros, Google, Safari e Internet Explorer;
- Proveedores de servicios de redes sociales: entidades que prestan servicios que conectan a dos usuarios finales a través de plataformas en línea, incluidos, entre otros, Facebook, LinkedIn e Instagram;
- Proveedores de servicios electrónicos: entidades que permiten a los usuarios finales comunicarse entre sí (por ejemplo, Outlook y los servicios de chat de juegos);
- Proveedores de servicios de distribución de aplicaciones: entidades que proporcionan acceso a servicios de aplicaciones, como Google (a través de Google Play Store) y Apple (a través de IOS App Store);
- Proveedores de servicios de alojamiento: entidades que permiten el alojamiento de materiales almacenados proporcionados en servicios de redes sociales, servicios electrónicos pertinentes o servicios de Internet designados, incluidos, entre otros, Apple y Microsoft, cada uno a través de su prestación de servicios en la nube;
- Empresas de desarrollo de hardware: entidades que crean, desarrollan y/o mantienen equipos tecnológicos, activos físicos y otros artículos tangibles;
- Empresas de desarrollo de software: entidades que crean, diseñan, desarrollan y mantienen programas, aplicaciones, marcos u otros componentes de software.

Estas empresas son intermediarias en los actos de VBG-FT y sus acciones (o inacción) son fundamentales para detener o amplificar los actos violentos. Aunque muchas plataformas y tecnologías en línea se construyeron para su "aplicación general", hay algunas "plataformas creadas a propósito" que se diseñaron deliberadamente para cometer y propagar actos de VBG-FT, como el abuso sexual basado en la imagen (IBSA) y la divulgación no consentida de imágenes íntimas y, por tanto, para beneficiarse de comportamientos abusivos[146]. Sin embargo, incluso las plataformas de aplicaciones genéricas contribuyen a amplificar la VBG-FT a través de características y modelos de negocio distintos que priorizan el crecimiento y los beneficios por encima de los derechos humanos, maximizan la participación de los usuarios y favorecen el contenido sensacionalista, y permiten la automatización de los abusos y el anonimato de los perpetradores[147]. Estas plataformas a menudo no responden a los casos de VBG-FT y, por ejemplo, suspenden las cuentas de las personas sobrevivientes en lugar de eliminar el material ofensivo y responsabilizar a los agresores. En otros casos permiten páginas que promueven contenidos misóginos mientras censuran a los usuarios que hablan del sexo y la comunidad LGBTQIA+ de una manera positiva. Además, las empresas tecnológicas suelen resistirse a abordar cuestiones de igualdad y reproducen la misoginia, el racismo y la discriminación en sus algoritmos. Por ejemplo, se ha demostrado que los sistemas comerciales de IA tienen importantes sesgos de género y de tipo de piel[148], lo que probablemente se deba a la falta de diversidad en el sector tecnológico. Los productos y servicios basados en algoritmos e IA perpetúan los prejuicios implícitos existentes en la sociedad y pueden dar lugar a una mayor discriminación, ya que se basan en los datos y la información disponibles y pueden estar basados en supuestos sesgados[149].

Sin una regulación clara, las empresas privadas de tecnología tienen poca obligación de abordar la VBG-FT mediante la eliminación de contenidos nocivos o la incorporación de funciones de seguridad como parte de la plataforma o la tecnología.

Las obligaciones de promover y proteger la seguridad de los usuarios finales son fundamentales para abordar eficazmente la VBG-FT. Aunque muchas empresas, en particular las plataformas de redes sociales han introducido la moderación de contenidos para identificar y eliminar los contenidos abusivos, el diseño y la aplicación de estas medidas no siempre ha tenido éxito y ha supuesto una carga adicional para las personas sobrevivientes y los usuarios individuales a la hora de detener el abuso. Además, estos mecanismos se basan en políticas y prácticas de "libertad de expresión" que incluyen muchas excepciones a lo que constituye abuso y discurso del odio, que son manipuladas por los perpetradores para silenciar a las personas sobrevivientes. La moderación de contenidos también es muy selectiva e incoherente, y las decisiones suelen estar sesgadas, determinadas por la opinión pública, la influencia política y los conflictos de intereses, lo que da lugar a la eliminación de contenidos inocuos, mientras que los contenidos abusivos no están prohibidos.150

Aunque la moderación de contenidos es un primer paso para detener la VBG-FT, las empresas tecnológicas y de plataformas deben hacer más para garantizar la seguridad en el uso de la tecnología y las plataformas en línea. Las empresas tecnológicas deben colaborar con los gobiernos y la sociedad civil para poner en marcha mecanismos que respondan y prevengan eficazmente la VBG-FT de una manera sensible al género y a la cultura, al tiempo que son transparentes y proactivas a la hora de abordar la VBG-FT desde el diseño de sus productos hasta la denuncia de casos y la gestión de sus datos.

1. United Nations Department of Economic and Social Affairs (2020). Shaping the Trends of Our Time. Report of the UN Economist Network for the UN 75th Anniversary. Disponible en: https://www.un-ilibrary.org/content/books/9789210053556
2. Ibid.
3. Flynn, A., Powell, A., and Hindes, S. (2021). Technology-facilitated abuse: a survey of support services stakeholders (Research report, 02/2021). ANROWS. Disponible en: https://20ian81kynqg- 38bl3l3e-h8bf-wpengine.netdna-ssl.com/wp-content/uploads/2021/07/4AP.4-Flynn_et_al-TFa_Stakeholder_Survey.pdf UNFPA, UN Women, Quilt.AI (2021). COVID-19 and violence against women: the evidence behind the talk. Disponible en: https://asiapacific.unfpa.org/en/publications/covid-19-and-violence-against-women-evidence-behind-talk?_ga=2.130256973.39170622.1628523607- 1469909938.1607087406
   UN Women, UNFPA (2021). Impact of COVID-19 on gender equality and women's empowerment in East and Southern Africa. Available at: https://data.unwomen.org/ publications/covid-19-gender-equality- east-and-southern-africa
4. Khoo, C. (2021). Deplatforming misogyny: report on platform liability for technology-facilitated gender-based violence. LEAF. Disponible en: https://www.leaf.ca/publica- tion/deplatforming-misogyny/
5. Amnistía Internacional (2018). Twitter intoxicado. Disponible en: https://www.amnesty. org/en/latest/news/2018/03/online-vio- lence-against-women-chapter-1/
6. Plan International (2020). Free to Be Online? Girls' and young women's experiences of online harassment. Disponible en: https:// plan-international.org/publications/free- tobeonline
7. Ibid.
8. Khoo, Deplatforming Misogyny.
9. E.L. Backe, P. Lilleston y J. McCleary-Sills, "Networked individuals, gendered violence: a literature review of cyber violence", Violence Gender, vol. 5, n.º 3, (2018), pp. 135-145.
   C. McGlynn, E. Rackley y R. Houghton, "Beyond 'revenge porn': the continuum of image-based sexual abuse", Feminist Legal Studies, vol. 15, (2017), pp. 1-22.
10. United Nations Human Rights Council, 20th Sess., Agenda item 3., U.N. Doc A/HRC/20/L.13 (29 Jun. 2012) United Nations (1948). Universal Declaration of Human Rights. Disponible en: https:// www.un.org/en/about-us/universal-dec- laration-of-human-rights [accessed 11 November 2021].
    UN General Assembly (1966). International Covenant on Civil and Political Rights, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171, Disponible en: https://www.ohchr.org/en/profes- sionalinterest/pages/ccpr.aspx [accessed 11 November 2021].
11. OHCHR (2018). Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective. Disponible en: https://www.ohchr.org/EN/Issues/Women/SRWomen/Pages/SRWomenIn- dex.aspx
12. Terminology and definitions that refer to TFGBV are multiple and diverse. See Part 4.
13. See glossary in Part 4 for definitions of technology-related terms.
14. Flavia Fascendini and Kateřina Fialová (2011). Voices from digital spaces: Technology related violence against women. Published by Association for Progressive Communications. Disponible en: https://www. apc.org/sites/default/files/APCWNSP_ MDG3advocacypaper_full_2011_EN_0.pdf
15. L., Sardinha y H.E. Nájera Catalán, "Attitudes towards domestic violence in 49 low- and middle-income countries: A gendered analysis of prevalence and country-level correlates", PloS One, vol. 13, n.º 10, (2018), e0206101. https://doi.org/10.1371/journal. pone.0206101
16. J. Bailey, N. Henry y A. Flynn, "Technology-Facilitated Violence and Abuse: Inter- national Perspectives and Experiences", en The Emerald International Handbook of Technology Facilitated Violence and Abuse,
    J. Bailey, A. Flynn y N. Henry, eds. (Bingley, Emerald Publishing Limited, 2021) pp. 1-17. https://doi.org/10.1108/978-1-83982-848- 520211001
17. Suzie Dunn y Kristen Thomasen, "Reasonable expectations of privacy in an era of drones and deepfakes- expanding the Supreme Court of Canada's decision in R v Jarvis", en The Emerald International Hand- book of Technology Facilitated Violence and Abuse, J. Bailey, A. Flynn y N. Henry, eds. (Bingley, Emerald Publishing Limited, 2021).
18. Webinar: Financial freedom - creating economic security and escaping financial abuse. National Summit on Women's Safety, September 2021. Disponible en: https://regonsite.eventsair.com/national-summit-on-womens-safety/
19. See Part 3 "Glossary of terms" for a more comprehensive list of forms of TFGBV and their definitions.
20. VAW Learning Network (2013). Technology-related Violence Against Women. Disponible en: http://www.vawlearningnetwork. ca/our-work/issuebased_newsletters/ issue-4/index.html
21. Flynn, Powell, and Hindes, Technology-facilitated abuse.
22. N. Henry and A. Powell, "Technology-facilitated sexual violence: a literature review of empirical research". Trauma, Violence & Abuse, vol. 19, No. 2, (2018), pp. 195–208. https://doi.org/10.1177/1524838016650189
23. Ibid.
24. Flynn, Powell, and Hindes, Technology-facilitated abuse. LGBTQI+ populations are particularly susceptible to online harassment and its harms, especially when it comes to threats and/or acts of public disclosure of their gender identity or sexual orientation that may happen with or without extortion and sextortion: S. Dunn (2020). Technology-Facilitated Gender- Based Violence: An Overview (Waterloo, ON: Centre for International Governance Innovation). Available at: https://apo.org.au/node/309987
25. VAW Learning Network, Technology-related violence against women.
26. Henry and Powell, Technology-facilitated sexual violence.
27. C. Parsons, A. Molnar, J. Dalek, J. Knockel, M. Kenyon, B. Haselton, C. Khoo and R. Deibert (2019) The Predator in Your Pocket: A Multi- disciplinary Assessment of the Stalker- ware Application Industry. The Citizen Lab. Disponible en: https://citizenlab.ca/2019/06/the-predator-in-your-pocket-a-multidisci-pli- nary-assessment-of-the-stalker-ware-appli- cation-industry/
28. Flynn, Powell, and Hindes, Technology facilitated abuse.
29. McGlynn, C., and Rackley, E., "Image-Based Sexual Abuse", Oxford Journal of Legal Studies, vol. 37, No. 3, (2017), pp. 534–561. https://doi.org/10.1093/ojls/gqw033
30. Flynn, Powell, and Hindes, Technology-facilitated abuse.
31. En 2019, durante una fiesta popular en España, un delincuente instaló cámaras ocultas en una zona pública con el fin de grabar imágenes de mujeres orinando -los hombres han sido eliminados de las grabaciones-. Estas imágenes, que mostraban los rostros y los órganos sexuales de las sobrevivientes, se subían después a sitios web pornográficos. Se identificó a más de 80 sobrevivientes, entre ellas menores. Este caso ha sido desestimado en los tribunales, lo que demuestra la limitada capacidad de

los sistemas judiciales para responder a los casos de VBG-FT. Sin embargo, mujeres activistas y sobrevivientes se han unido a un movimiento para reclamar sus derechos y han contribuido a identificar casos similares en otras partes del país. El País (2021). Revuelta en Galicia contra las cámaras ocultas que denigran a las mujeres. Disponible en: https://elpais.com/sociedad/2021-04-04/revuelta-en- galicia-contra-las-camaras-ocultas-que- denigran-a-las-mujeres.html

32. Henry and Powell, Technology-facilitated sexual violence. N. Henry, A. Flynn and A. Powell, "Technology-facilitated domestic and sexual violence: a review", Violence Against Women, vol. 26, No. 15–16, (2020), pp. 1828–1854. https://doi.org/10.1177/1077801219875821
33. Ibid.
34. Henry and Powell, Technology-facilitated sexual violence. Henry, Flynn and Powell, Technology-facilitated domestic and sexual violence.
35. Henry, Flynn and Powell, Technology-facilitated domestic and sexual violence.
36. S. Craven, S. Brown and E. Gilchrist, "Sexual grooming of children: review of literature and theoretical considerations", Journal of Sexual Aggression, vol. 12, (2006), pp. 287–299, 10.1080/13552600601069414
37. M.A. Franks, "Sexual harassment 2.0", Mary- land Law Review, vol. 71, p. 2012655.
38. J.M. MacAllister, the doxing dilemma: seeking a remedy for the malicious publication of personal information. Fordham Law Review, vol. 85, (2017), pp. 2451–2383.
39. S. Eckert and J. Metzger-Riftkin (2020). Doxxing. The International Encyclopedia of Gender, Media, and Communication. https://doi.org/10.1002/9781119429128.iegmc009
40. D. Douglas, "Doxing: a conceptual analysis", Ethics Information Technology, vol. 18, (2016), pp. 199–210.
41. MacAllister, The doxing dilemma.
42. VAW Learning Network, Technology-related violence against women.
43. N. Henry and A. Powell, "Sexual violence in the digital age: the scope and limits of criminal law", Social & Legal Studies, vol. 25, No. 4, (2016), pp. 397–418. doi:10.1177/0964663915624273
44. Flynn, Powell y Hindes, Technology-facilitated abuse.
45. Fascendini y Fialová, Voices from digital spaces (véase la nota 14).
46. VAW Learning Network, Technology-related violence against women.
47. Fascendini y Fialová, Voices from digital spaces (véase la nota 14).
48. APC (2020). El uso de la tecnología para perpetrar la violencia hacia las mujeres y combatirla. Disponible en: https://www. apc.org/en/pubs/research/how-technol-ogy-being-used-perpetrate-violence-agai
49. Nicki Dell, Karen Levy, Damon McCoy y Thomas Ristenpart (2018). How domestic abusers use smartphones to spy on their partners. Disponible en: https://www.vox. com/the-big-idea/2018/5/21/17374434/intimate-partner-violence-spy-ware-domestic-abusers-apple-google
Parsons, Molnar, Dalek, Knockel, Kenyon, Haselton, Khoo and Deibert, The predator in your pocket.
50. 5Save the Children (2021). India: girls in India facing greater online risk of child marriage and trafficking during pandemic. Disponible en: https://www.savethechildren.net/news/india-girls-india-facing-greater-online-risk- child-marriage-and-trafficking-during-pan- demic
51. Gulfer Ulas (2019). Female Radicalisa- tion: Why do Women join ISIS? LSE Middle East Centre. Disponible en: https://blogs.lse.ac.uk/mec/2019/08/15/female-radicalisation-why-do-women-join-isis/
Lisa Blaker, "The Islamic State's use of online social media", Military Cyber Affairs, vol. 1, No. 1, (2015), p. 4. Disponible en: https://digitalcommons.usf.edu/cgi/viewcontent.cgi?article=1004&context=mca
52. A. Van der Wilk (2018). Cyber violence and hate speech online against women. Study for the FEEM Committee. Disponible en: https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604979/IPOL_STU(2018)604979_EN.pdf
53. A. Gurumurthy, A. Vasudevan and N. Chami (2019). Born digital, Born free? A socio-le- gal study on young women's experiences of online violence in South India. Bangalore, India: IT for Change. Disponible en: https:// itforchange.net/sites/default/files/1662/ Born-Digital_Born-Free_SynthesisReport. pdf
54. D. Freed, J. Palmer, D.E. Minchala, K. Levy, T. Ristenpart and N Dell, "Digital technologies and intimate partner violence: a qualitative analysis with multiple stakeholders", Proceedings of the ACM on Human-Computer Interaction, vol. 1, (2017), pp. 1–22, https://doi.org/10.1145/3134681
55. D.K . Citron, Hate Crimes in Cyberspace (Cambridge, MA: Harvard University Press, 2014).
J. West, *Cyber-Violence Against Women* (Vancouver, BC: Battered Women's Support Services, 2014). www.bwss.org/wp-con- tent/uploads/2014/05/CyberVAWReport- JessicaWest.pdf
56. Safety Net Canada, *Assessing Technology in the Context of Violence Against Women & Children: Examining Benefits & Risks (Vancouver, BC:* Safety Net Canada, 2013). https://bcsth.ca/wp- content/uploads/2016/10/Assessing-Technology-in-the-Context-of-Violence-AgainstWomen-Children.-Examining-Benefits-Risks.pdf.
57. Dunn, Technology-facilitated gender-based violence: an overview; Although technology and digital tools have been used in humanitarian contexts to support programmes and improve response, they also have the potential to exacerbate conflict and to increase the risk of intended and unintended harm to affected populations. State and non-State actors can misuse technology to perpetrate violence and cause further harm to the population, and practices by humanitarian actors – particularly regarding data protection – may leave vulnerable populations at increased risk. Más en: https://blogs.icrc.org/law-and-policy/2019/06/12/digital-risks-populations-armed-conflict-five-key-gaps-humanitarian-sector/
58. UN (2019). United Nations Strategy and Plan of Action on Hate Speech. Disponible en: https://www.un.org/en/genocideprevention/hate-speech-strategy.shtml
59. Dunn, Technology-facilitated gender-based violence: an overview.
60. Douglas, Doxing: a conceptual analysis. Dunn, Technology-facilitated gender-based violence: an overview.
61. Dunn, Technology-facilitated gender-based violence: an overview.
62. K. Levy and B. Schneier, "Privacy threats in intimate relationships", Journal of Cyber- security (Oxford), vol. 6, No. 1, (2020),https://doi.org/10.1093/cybsec/tyaa006 D. Freed, J. Palmer, D. Minchala, K. Levy, T. Ristenpart and N. Dell, "'A stalker's
63. L. Hinson, L. O'Brien-Milne, J. Mueller, V. Bansal, N. Wandera y S. Bankar (2019). Defining and Measuring Technol- ogy-facilitated Gender-based Violence (Washington DC: Centro Internacional de Investigación sobre la Mujer). Disponible en: http:// www.svri.org/sites/default/files/attachments/2019-03-25/ICRW_VBG-FT-Market- ing_Brief_v3_WebReady_0.pdf
64. Los países incluidos son Alemania, Arabia Saudí, Argelia, Argentina, Australia, Bangladesh, Bélgica, Brasil,

Canadá, Chile, China, Colombia, Egipto, Corea del Sur, España, Estados Unidos, Filipinas, Francia, Ghana, Guatemala, India, Indonesia, Italia, Japón, Kazajstán, Malasia, Marruecos, México, Myanmar, Países Bajos, Nigeria, Pakistán, Perú, Polonia, Reino Unido, Rumanía, Rusia, Sudáfrica, Tailandia, Taiwán, Tanzania, Turquía, Ucrania, Venezuela y Vietnam.
65. Economist Intelligence Unit (2021). Measuring the prevalence of online violence against women. Disponible en: https://online- violencewomen.eiu.com/
66. Plan International, ¿Libres para estar en línea? (véase la nota 6).
67. Ibid.
68. OMS (2021). Global, regional and national estimates for intimate partner violence against women and global and regional estimates for non-partner sexual violence against women. Disponible en: https://www. who.int/news/item/09-03-2021-devas- tatingly-pervasive-1-in-3-women-globally- experience-violence
69. M. Duggan (2017). Online Harassment 83 2017. Pew Research Centre. Disponible en: https://www.pewresearch.org/inter- net/2017/07/11/online-harassment-2017/
70. Dunn, Technology-facilitated gender-based violence: an overview.
71. Plan International, ¿Libres para estar en línea? (véase la nota 6).
72. Ibid.
73. Children's Society, Young Minds (2018). Safety net: cyberbullying's 85 impact on young people's mental health: Inquiry report summary. Disponible en: https://www.youngminds.org.uk/media/gmvdnzcv/executive-summary-pcr144a_social_media_cyberbullying_ inquiry_summary_report.pdf
74. Pew Research Centre (2018). Teens, social media and Technology 2018. Disponible en: https://www.pewresearch.org/inter- net/2018/05/31/teens-social-media-tech- nology-2018/
75. The World Wide Web Foundation (2020). IWF 2020 Annual Report | Face the facts. Disponible en: https://www.iwf.org.uk/report/ iwf-2020-annual-report-face-facts
76. Janine M. Zweig, Meredith Dank, Pamela Lachman y Jennifer Yahner, Technol- ogy, Teen Dating Violence and Abuse, and Bullying (Washington DC: Urban Insti- tute, 2013). Disponible en: https://www. urban.org/sites/default/files/publica- tion/23941/412891-Technology-Teen-Dat- ing-Violence-and-Abuse-and-Bullying.PDF.
77. Plan International, ¿Libres para estar en línea? (véase la nota 6).
78. Fundación World Wide Web (2020). The online crisis facing women and girls threatens global progress on gender equality. Disponible en: https:// webfoundation.org/2020/03/the-online- crisis-facing-women-and-girls-threatens- global-progress-on-gender-equality/
79. Plan International, ¿Libres para estar en línea? (véase la nota 6).
80. The Wall Street Journal (2021). The Face- book files: Facebook knows Instagram Is toxic for teen girls, company documents show. By Georgia Wells, Jeff Horwitz and Deepa Seetharaman. Available at: https:// www.wsj.com/articles/facebook-knows- instagram-is-toxic-for-teen-girls-company- documents-show-11631620739?mod=hp_lead_pos7&mod=article_inline
81. Amnistía Internacional, Twitter Intoxicado (véase la nota 5).
82. Dunn, Technology-facilitated gender-based violence: an overview (véase la nota 24).
83. J. Posetti, N. Shabbir, D. Maynard, K. Bontcheva y N. Aboulez (2021). The chilling: global trends in online violence against women journalists. UNESCO. Disponible en: https://en.unesco.org/news/unesco-re- leases-pioneering-discussion-paper-on- line-violence-against-women-journalists
84. Inter-Parliamentary Union (2016). Sexism, harassment and violence against women parliamentarians
85. R. Lewis, M. Rowe y C. Wiper, "Online abuse of feminists as an emerging form of violence against women and girls", British Journal of Criminology, vol. 57, n.º 6, (2017), pp. 1462-1481. https://doi.org/10.1093/ bjc/azw073
86. Plan International ¿Libres para estar en línea? (véase la nota 6).
87. Dunn, Technology-facilitated gender-based violence: an overview (véase la nota 24).
88. Amnistía Internacional, Twitter Intoxicado (véase la nota 5).
89. Plan International ¿Libres para estar en línea? (véase la nota 6).
90. Dunn, Technology-facilitated gender-based violence: an overview (véase la nota 24).
91. Delfina Schenone Sienra and Mariana Palumbo (2017). EROTICS Global Survey 2017: Sexuality, rights and internet regulations. Association for Progressive Communications. Available at: https://www.apc. org/sites/default/files/Erotics_2_FIND-2. pdf
92. Stonewall (2017). LGBT in Britain – Hate Crime and Discrimination. Available at: https://www.stonewall.org.uk/lgbt-britain-hate-crime-and-discrimination
93. Lewis, Rowe and Wiper, Online abuse of feminists as an emerging form of violence against women.
94. OHCHR (2018). Report of the Special Rapporteur on violence against women (veáse la nota 11).
95. A. Marganski and L. Melander, "Intimate partner violence victimization in the cyber and real world: examining the extent of cyber aggression experiences and its association with in-person dating violence", Journal of Interpersonal Violence, vol. 33, No. 7, (2018), pp. 1071–1095. https://doi.org/10.1177/0886260515614283
96. Flynn, Powell, and Hindes, Technology-facilitated abuse.
97. Daxton, C. (2014). Virtual World, Real Fear. Women's Aid report into online abuse, harassment and stalking. Disponible en: https://www.womensaid.org.uk/wp-con- tent/uploads/2015/11/Women_s_Aid_ Virtual_World_Real_Fear_Feb_2014-3.pdf
98. Dunn, Technology-facilitated gender-based violence: an overview (véase la nota 24).
99. D.F. Malanga (2020). Tackling Gender-based Cyber Violence against Women and Girls in Malawi amidst the COVID-19 Pandemic. Disponible en: https://africanin- ternetrights.org/sites/default/files/Donald_ Flywell-1.pdf
100. Serie de aprendizaje sobre la violencia basada en el género facilitada por la tecnología violencia basada en el género - GBV AoR Helpdesk. Resumen de Aprendizaje 1: Comprendiendo la violencia basada en el género facilitada por la tecnología.
101. Ibid.
102. Amnistía Internacional, Twitter Intoxicado (véase la nota 5).
103. Gurumurthy, Vasudevan and Chami, Born digital, born free?? (véase la nota 53).
104. Plan International ¿Libres para estar en línea? (véase la nota 6).
105. Dunn, Technology-facilitated gender-based violence: an overview (véase la nota 24).
S. Bates, "Revenge porn and mental health: a qualitative analysis of the mental health effects of revenge porn on female survivors", Feminist Criminology, vol. 12, n.º 1, (2017), pp. 22-42. https://doi. org/10.1177/1557085116654565
106. C. McGlynn, E. Rackley, N. Henry, N. Gavey, A. Flynn y A. Powell, "'It's torture for the soul': the harms of image-based sexual abuse", Social and Legal Studies, vol. 30, nº 4, (2021), pp. 541-562.
107. Malanga, Tackling gender-based cyber violence.

108. GBV AoR Helpdesk (2021). Learning Series on Technology-Facilitated Gender-Based Violence. Learning Brief 3: Implications of technology-facilitated GBV and actions for humanitarian agencies, donors and online industries.
109. Plan International, ¿Libres para estar en línea? (véase la nota 6).
110. Dunn, Technology-facilitated gender-based violence: an overview (véase la nota 24).
111. Flynn, Powell and Hindes, Technology-facilitated abuse.
112. Malanga, Tackling gender-based cyber violence.
113. Plan International, ¿Libres para estar en línea? (véase la nota 6).
114. Amnistía Internacional, Twitter Intoxicado (véase la nota 5).
115. Dunn, Technology-facilitated gender-based violence: an overview (véase la nota 24).
116. Malanga, Tackling gender-based cyber violence.
117. Plan International, ¿Libres para estar en línea? (véase la nota 6).
118. Dunn, Technology-facilitated gender-based violence: an overview (véase la nota)
119. Serie de aprendizaje sobre la violencia basada en el género facilitada por la tecnología violencia basada en el género - GBV AoR Helpdesk 2022 (véase la nota 108).
120. Dunn, Technology-facilitated gender-based violence: an overview (véase la nota 24).
121. Serie de aprendizaje sobre la violencia basada en el género facilitada por la tecnología violencia basada en el género - GBV AoR Helpdesk 2022 (véase la nota 108).
122. Wall Street Journal, The Facebook files (véase la nota 80).
123. Flynn, Powell and Hindes, Technology-facilitated abuse.
124. Ibid.
125. Parsons, Molnar, Dalek, Knockel, Kenyon, Haselton, Khoo y Deibert, The Predator in Your Pocket (véase la nota 27).
126. Freed, Palmer, Minchala, Levy, Ristenpart y Dell, A stalker's paradise (véase la nota 62).
127. Freed, Palmer, Minchala, Levy, Ristenpart y Dell, Digital technologies, and intimate partner violence (véase la nota 54).
128. C. Laxton (2014). Virtual World, Real Fear. Women's Aid report into online abuse, harassment and stalking. Disponible en: https://www.womensaid.org.uk/wp-con- tent/uploads/2015/11/Women_s_Aid_ Virtual_World_Real_Fear_Feb_2014-3.pdf
129. Dunn, Technology-facilitated gender-based violence: an overview (véase la nota 24).
130. https://www.gbvims.com/
131. Dada la creciente digitalización de los servicios de salud, por ejemplo, existe un mayor riesgo de que se produzcan problemas de privacidad y confidencialidad de los datos e infracciones en la protección de estos. De hecho, la OMS ha informado que, aunque el 70% de los 113 países encuestados contaban con legislación relativa a los derechos básicos de privacidad, sólo el 30% de ellos disponía de legislación sobre la privacidad de las historias clínicas electrónicas. Incluso menos países contaban con marcos jurídicos para las historias clínicas electrónicas que abordaran algo más que la privacidad. La falta de políticas y marcos jurídicos sobre temas como la propiedad, la confidencialidad y la seguridad de los datos se ha identificado como un importante obstáculo para la ampliación de las historias clínicas electrónicas. Organización Mundial de la Salud (2012). Legal frameworks for eHealth: based on the findings of the second global survey on eHealth. (Global Observatory for eHealth Series, v.5). Disponible en: https://www.who.int/goe/publications/legal_framework_web.pdf
132. Alisha C. Salerno-Ferraro, Caroline Erentzen y Regina A. Schuller, "Young women's experiences with technology-facilitated sexual violence from male strangers", Jour- nal of Interpersonal Violence, (2021), https:// doi.org/10.1177/08862605211030018
133. eSafety Commission Australia. Online
134. Plan International, ¿Libres para estar en línea? (véase la nota 6).
135. Ibid.
136. Amnistía Internacional, Twitter Intoxicado (véase la nota 5).
137. UNICEF Asia Oriental y Pacífico (2021). What we know about the gender digital divide for girls: a literature review. Disponible en: https://www.unicef.org/eap/reports/inno- vation-and-technology-gender-equality-0
138. Economist Intelligence Unit, Measuring the prevalence of online violence (véase la nota 65).
139. Khoo, Deplatforming misogyny (véase la nota 4).
140. Ibid.
141. Oltermann, P. 5 de enero de 2018. Una nueva y dura ley alemana pone a las empresas tecnológicas y la libertad de expresión en el punto de mira. Disponible en: https:// www.theguardian.com/world/2018/ jan/05/tough-new-german-law-puts-tech-firms-and-free-speech-in-spotlight
142. Khoo, Deplatforming misogyny (véase la nota 4).
143. Ibid.
144. Comisario de eSafety. Disponible en: https:// www.esafety.gov.au/ [consultado el 4 de noviembre de 2021].
145. Ley de seguridad en línea de 2021 (Cth). Nº 76, 2021. (Austl.)
146. Khoo, Deplatforming misogyny (véase la nota 4).
147. Ibid.
148. Larry Hardesty (2018). Study finds gender and skin-type bias in commercial artificial-intelligence systems. Disponible en: https://news.mit.edu/2018/ study-finds-gender-skin-type-bias-artifi- cial-intelligence-systems-0212
149. Rebecca Heilweill (2020). Por qué los algoritmos pueden ser racistas y sexistas. Disponible en: https://www.vox .c om/recode/2020/2/18/21121286/algorithms-bias-discrimination-facial-recognition-transparency
Brian Resnick (2019). Sí, la inteligencia artificial puede ser racista. Disponible en: https://www.vox.com/ science-and-health/2019/1/23/18194717/ alexandria-ocasio-cortez-ai-bias
150. Khoo, Deplatforming misogyny (véase la nota 4).

Parte 2

Recomendacione y estrategias para VBG-FT

Prevención y Respuesto


es

Los esfuerzos de prevención y respuesta requieren el esfuerzo colectivo de los gobiernos nacionales y las empresas tecnológicas privadas, incluidas las empresas de plataformas, dadas las características específicas de la VBG-FT, sus nuevas formas y su constante evolución. Esto debe guiarse por enfoques basados en los derechos humanos, teniendo en cuenta las experiencias de las mujeres y las niñas en toda su diversidad, para garantizar que la reforma y la regulación para prevenir y responder a la VBG-FT satisfacen sus necesidades.

A continuación, se presenta una lista no exhaustiva de recomendaciones para que los Estados y las empresas privadas de tecnología aborden la creciente prevalencia e impacto de la VBG-FT. Estas recomendaciones requieren una inversión significativa y sostenida de recursos financieros, técnicos y humanos por parte de entidades nacionales e internacionales, gobiernos y sector privado.

También requieren alianzas sólidas entre empresas privadas de tecnología, gobiernos, movimientos feministas y de derechos digitales, proveedores de servicios de VBG, académicos y, por último y más importante, sobrevivientes de la VBG-FT.

1 Recomendaciones para los Gobiernos Nacionales

Política y legislación

La legislación y las políticas deben configurarse dentro de un marco de derechos humanos que aborde la discriminación estructural, la violencia y las desigualdades a las que se enfrentan las mujeres. Los marcos jurídicos deben proteger adecuadamente todos los derechos humanos de las mujeres en línea, incluido el derecho a una vida libre de violencia, la libertad de expresión, el acceso a la información, el derecho a la intimidad y a la protección de datos.[151] Además de reforzar la rendición de cuentas de los perpetradores, las leyes deben regular las empresas privadas de tecnología para que apliquen mecanismos de seguridad y respuesta que prevengan y mitiguen la aparición de la VBG-FT.

La política y la legislación deben desarrollarse con la plena participación y consulta de las personas sobrevivientes de la VBG-FT, los proveedores y servicios de primera línea, así como académicos y expertos sustantivos en los campos de la regulación de plataformas, la moderación de contenidos y la rendición de cuentas algorítmica.

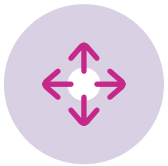
- Reconocimiento e integración de la VBG-FT en las leyes, normativas y políticas civiles y penales para regular las empresas privadas de tecnología y exigir la rendición de cuentas de los infractores.
- Establecer un órgano estatutario independiente para abordar la VBG-FT con un mandato que puede incluir lo siguiente: (a) poderes para administrar recursos legales y apoyo a las personas afectadas por la VBG-FT en plataformas digitales; (b) poderes reguladores y coercitivos sobre las empresas privadas de tecnología para integrar mecanismos de seguridad y eliminar inmediatamente los contenidos nocivos; (c) avanzar en la investigación sobre VBG-FT para apoyar leyes y políticas basadas en evidencias; (d) promover y facilitar la eliminación de contenidos nocivos tras la denuncia de las víctimas o de los proveedores de servicios de primera línea; (e) proporcionar formación y educación al público, a las partes interesadas pertinentes y a los profesionales; y (f) apoyar las alianzas con empresas privadas de tecnología para permitir el cumplimiento de los requisitos de seguridad obligatorios o voluntarios.
- Cuando se introducen nuevas leyes y políticas, se presupuestan adecuadamente para garantizar su implementación y se proporciona a las autoridades competentes y al poder judicial la formación y los conocimientos necesarios.
- Las leyes deben exigir la provisión de soluciones rápidas, prácticas y accesibles para las VBG-FT, incluido el apoyo a espacios de moderación accesibles para apelar la negativa a retirar los materiales ofensivos.
- Exigir el refuerzo de los sistemas de apoyo a la seguridad de los datos, incluida la información confidencial recopilada y gestionada por el Estado y los datos recogidos a través de aplicaciones y plataformas basadas en la localización.
- Deben establecerse acuerdos internacionales y un marco legislativo común para luchar contra la VBG-FT transfronteriza. A menudo, los perpetradores no rinden cuentas debido a problemas trans-jurisdiccionales, ya que cometen los abusos desde distintos Estados o países.

En la regulación de las empresas privadas de tecnología:

- Establecer y aplicar leyes y reglamentos que obliguen a las empresas privadas de tecnología a desarrollar, mantener e implementar políticas para responder a la VBG-FT y mitigar sus efectos mediante una serie de procesos que incluyan lo siguiente: (1) mecanismos visibles, de fácil acceso y en un lenguaje sencillo para denunciar quejas y abusos de contenidos nocivos; (2) eliminación **inmediata** de los contenidos nocivos denunciados (manteniendo registros con fines probatorios); (3) mecanismos de moderación eficaces; (4) exigir la formación de todo el personal para que comprenda su papel en el monitoreo y eliminación de contenidos nocivos relacionados con la VBG-FT; y (5) realización de auditorías independientes y publicación de informes anuales exhaustivos de transparencia relativos a la implementación de las políticas.
- Garantizar una regulación que apoye la retirada inmediata de contenidos nocivos definidos de una plataforma sin necesidad de recurrir a una orden judicial, costos y otros retos asociados y legales.[152]
- Cuando se dicte una orden contra una empresa de plataforma, asegúrese de que exige la retirada de los contenidos de cualquiera de las empresas de plataforma matrices, filiales o hermanas de dicha plataforma en las que también aparezcan los mismos contenidos.[153]
- Considerar la posibilidad de ofrecer incentivos a las empresas tecnológicas privadas para fomentar el cumplimiento y la promoción activa de la protección de las mujeres y niñas que utilizan sus servicios.
- La publicidad, la venta y la distribución de aplicaciones y dispositivos comercializados con fines de monitoreo deben controlarse cuidadosamente y solo deben permitirse para fines concretos. También debe restringirse su acceso, incluso eliminándolos de las tiendas oficiales de aplicaciones.

Mecanismos de respuesta reforzados

Es fundamental realizar inversiones sostenidas y profundas en mecanismos de respuesta centrados en las personas sobrevivientes y con una perspectiva feminista que aborden todas las formas de VBG-FT, tanto como incidente aislado como parte de un patrón de conducta.



- Garantizar enfoques participativos y feministas en el diseño de leyes, políticas, mecanismos de respuesta reforzados y materiales de formación asociados para captar la amplitud de la experiencia de las personas sobrevivientes.
- Reforzar los servicios de respuesta integral a la VBG-FT centrados en la sobreviviente mediante la formación continua y el desarrollo de capacidades de los proveedores de servicios de todos los sectores (incluidos los funcionarios encargados de hacer cumplir la ley, el poder judicial, los trabajadores sociales especializados en VBG, los proveedores de servicios de salud y psicosociales, los trabajadores sociales y de vivienda) para apoyar la identificación, la respuesta y la intervención temprana segura y centrada en la sobreviviente de la VBG-FT.
- Implicar a las entidades profesionales, incluidos los destinados a apoyar a periodistas y políticos, para que ofrezcan un espacio de colaboración entre las asociaciones profesionales y los servicios de respuesta a la VBG-FT.
- Garantizar la integración de las empresas privadas de tecnología en los mecanismos de remisión o derivación existentes de los responsables de primera línea de la respuesta a la VBG para garantizar una respuesta activa e inmediata a la VBG-FT mediante una serie de mecanismos, entre los que se incluyen apoyo a un servicio intermedio con capacidad para facilitar el acceso a los servicios de primera línea de respuesta a la VBG a los puntos focales de las empresas tecnológicas privadas.
- Recursos financieros, humanos y técnicos para los trabajadores de apoyo de primera línea y las organizaciones de base comunitaria, a fin de permitir respuestas inmediatas y eficaces con el pleno apoyo de los servicios de salud, sociales, policiales y jurídicos, incluidas las empresas privadas de tecnología.
- Garantizar que los refugios y espacios seguros cuenten con la seguridad necesaria (física y en línea) para garantizar la confidencialidad del lugar.
- Garantizar que todos los actores del sistema de justicia reciban la formación y los recursos necesarios para garantizar un alto nivel de experiencia y familiaridad con las tecnologías de la información y la comunicación y su funcionamiento, así como con las evidencias digitales, a fin de garantizar que se recojan, conserven y valoren debidamente las evidencias adecuadas y evitar la re-victimización de las personas sobrevivientes durante los procedimientos judiciales.[154]

Inversión en prevención

La prevención de la VBG-FT requiere trabajar con individuos y grupos de sobrevivientes, defensores y activistas, proveedores de servicios de VBG, así como con empresas privadas, departamentos y organizaciones públicas y gubernamentales y asociaciones profesionales. Una estrategia y un enfoque fundamentales para apoyar y mantener los esfuerzos de prevención serán la función de convocatoria del gobierno nacional para crear y mantener estas asociaciones.

Educación

- Invertir para mejorar la alfabetización digital de las adolescentes, las mujeres, en particular las de mayor edad, los activistas y los profesionales en toda su diversidad, mediante la oferta de cursos o talleres accesibles y gratuitos que puedan integrarse en la escuela, la universidad y las instituciones de formación profesional, los lugares de trabajo y los espacios comunitarios.
- Integración de módulos y conceptos en los planes de estudio y los paquetes de formación (incluida la educación integral de la sexualidad) para apoyar comportamientos e interacciones saludables en línea.[155]
- Desarrollo de planes de estudio y formación accesibles para que los centros educativos y los servicios comunitarios ofrezcan formación a los miembros de la comunidad de todas las edades y en toda su diversidad.
- Proporcionar acceso a servicios de apoyo a los miembros de la comunidad y, en particular, a las mujeres en toda su diversidad a la hora de navegar por la tecnología y los espacios en línea.
- Desarrollo de herramientas de apoyo a las mujeres en toda su diversidad, a los padres y a los educadores para que puedan proteger la privacidad en línea de niños y estudiantes.
- Continuar y ampliar el trabajo para garantizar que los programas de prevención de la VBG incluyan la participación de hombres y niños en la transformación de las masculinidades nocivas para abordar los comportamientos en línea.
- Inversión en evaluaciones de programas de educación y prevención para determinar la eficacia en el cambio de actitudes y comportamientos en línea.

Apoyar la acción y la incidencia comunitaria

- Promover la creación de espacios para grupos de pares vulnerables a la VBG-FT como red de apoyo esencial. Entre los ejemplos de grupos de apoyo por pares que han tenido éxito se encuentran los dirigidos por mujeres periodistas[156].
- Promover y proteger la voz de las mujeres y su participación segura en línea, fomentando comportamientos de apoyo y dotando a mujeres y niñas de las habilidades necesarias para contrarrestar los abusos.
- Apoyar activamente a las activistas y defensoras feministas, a las defensoras de los derechos humanos de las mujeres, a las periodistas y a las políticas que mantienen una presencia en línea para que sigan relacionándose con el público a través de este medio sin miedo a la VBG-FT mediante la creación de redes de pares (donde aún no existan) y facilitando la moderación proactiva de contenidos por parte de las empresas privadas de tecnología.

Seguridad de los datos

- Recursos dedicados a elaborar y aplicar leyes, políticas, sistemas y procesos, así como personal capacitado para garantizar la seguridad de los datos confidenciales.
- Recursos que permitan a los proveedores de servicios de primera línea seguir recopilando y protegiendo de forma segura los datos relativos a las personas sobrevivientes de VBG. Esto es fundamental dado el continuo de violencia en línea y fuera de línea, particularmente en el contexto de la VPI.

Datos e investigación

Es necesario reforzar los datos y la investigación para sentar las bases para desarrollar políticas, programas, leyes y estrategias de incidencia. Es fundamental comprender las formas de VBG-FT, sus repercusiones, los principales objetivos y perpetradores, así como las soluciones necesarias y deseadas y los mecanismos adecuados de rendición de cuentas.

- Es necesario desarrollar definiciones y terminología globales y estandarizadas de la VBG-FT y sus diferentes formas, tácticas y comportamientos asociados.
- Inclusión de la VBG-FT como forma o experiencia de violencia en las encuestas poblacionales estandarizadas[157], incluyendo, por ejemplo, la metodología de Estudio multipaís de la OMS o la Encuesta de Demografía y Salud, que se utilizan para determinar la prevalencia de la VBG. Para ello, es necesario desarrollar, probar y adaptar medidas estandarizadas de la VBG-FT, incluidas todas sus formas, en todos los contextos y culturas.
- Garantizar la inclusión de la VBG-FT como forma de violencia en los sistemas de datos administrativos sobre VBG. Esto puede requerir, por ejemplo, la modificación de los formularios de admisión y la documentación de gestión de casos para registrar el contexto (en línea o fuera de línea) en el que tuvo lugar la violencia. Esto permitirá comprender mejor cómo se denuncian, remiten y gestionan los casos de VBG-FT, así como analizar las tendencias, todo lo cual puede servir de base para la incidencia y las intervenciones basadas en evidencias.
- Mayor atención y concentración en la generación de investigación para determinar "qué funciona" para prevenir y responder a la VBG-FT.
- Recurrir a investigaciones empíricas, interdisciplinares y jurídico-políticas en profundidad realizadas por especialistas, expertos y organizaciones comunitarias de VBG-FT y las repercusiones de las nuevas tecnologías en las personas que sufren VBG-FT en todas las edades e interseccionalidades. Por ejemplo, el apoyo a la investigación para prevenir los abusos en comunicaciones cifradas.[158]

GOVERNO DO DISTRITO DE CHICUALACUALA

SERVIÇO DISTRITAL DE SAÚDE, MULHER E ACÇÃO SOCIAL

PROGRAMA DE VIOLÊNCIA BASEADA NO GÊNERO

Nº DE ORDEM	DATAS	ACTIVIDADE	RESPONSABILIDADE
01	01/12/20	Realização de palestras de sensiblização e conaciencialização sobre a Violência Baseada no Género	Ponto focal de VBG
02	08/12/20	Encontro de Coordenação Multisectorial de Atendimento Integrado a Violência Baseada no Género	Mecanismo Multissectorial
03	15/12/20	Realização de Supervisão e Apoio Técnico	Ponto focal de VBG
04	22/12/20	Sessões de debates radiofónicos sobre a Violência Baseada no Género	Ponto focal de VBG
05	29/12/20	Realização de visitas domiciliares a famílias vítimas de Violência Baseada no Género	Ponto focal de VBG

Chicualacuala, 01 de Dezembro de 2020

Salomão Gonçalves Matavele

/Tec. Sup. de Saúde N1/

LINHAS DE DENÚN

86 274 33 94-

87 542 43 68-

86 872 10 91-

República de Moçambique
MINISTÉRIO DA SAÚDE
cção Nacional de Saúde Pública
Nacional de Controlo da Tuberculose

para acabar
uberculose

SE TEM CURA.

Tosse há ma
de 2 seman
pode
Tubero

Cof Cof Cof Cof Cof

Vá a de
Sa nais
na.

teste.

2 Recomendaciones para Empresas Tecnológicas Privadas

Las empresas privadas deben reconocer su papel en la VBG-FT, crear y alimentar asociaciones productivas y a largo plazo con proveedores de servicios de VBG, mujeres en toda su diversidad, asociaciones profesionales, académicas y gobiernos nacionales para apoyar mecanismos de seguridad informados, eficaces e inmediatos que respondan inmediatamente, protejan y promuevan el derecho de las mujeres y las niñas a estar libres de violencia tanto en línea como fuera de ella.

- El desarrollo y la aplicación de tecnologías y plataformas digitales deben realizarse en colaboración y con la participación de las mujeres en toda su diversidad, así como de organizaciones y defensores[159], para garantizar unas características de seguridad y unos mecanismos de denuncia fiables y accesibles.
- La prevención, mitigación y respuesta a la VBG-FT deben incluirse en los Procedimientos Operativos Estándar de las plataformas de las redes sociales y las empresas tecnológicas para garantizar la eliminación inmediata de los contenidos nocivos, la moderación activa y las medidas de mitigación de la VBG-FT.
- Los mecanismos de denuncia deben garantizar una respuesta inmediata y la retirada del material perjudicial, a la espera de una investigación más exhaustiva de acuerdo con las políticas de buenas prácticas, así como la retirada del material de todas las filiales y sitios asociados.
- Garantizar políticas de modificación de contenidos, respuestas claras y transparentes.
- La seguridad debe incorporarse en la fase de diseño. Para una orientación y recomendaciones prácticas, véase el informe de resultados y recomendaciones "Tech Policy Design Lab: Online Gender-Based Violence and Abuse", que se basa en los resultados de una serie de talleres con las partes interesadas, incluidas las personas sobrevivientes de la VBG-FT y las empresas tecnológicas.[160]
- Puntos focales designados dentro de la empresa, disponibles en todo momento, para atender las denuncias y retirar el material ofensivo e infractor.
- Exigir que todo el personal de las empresas y plataformas tecnológicas de nueva creación participe en cursos de formación para mejorar la comprensión de la VBG-FT y su papel en el monitoreo y eliminación de contenidos nocivos.

151. Michael Geist (2021). Seguimiento de la submissions: what the government heard in its online-harms-consultation (since it-refuses-to-post-them). Disponible en: https://www.michaelgeist.ca/2021/10/ tracking-the-submissions-what-the-gov- ernment-heard-in-its-online-harms-con- sultation-since-it-refuses-to-post-them/
152. H. Young y E. Laidlaw (2020). Creating a Revenge Porn Tort for Canada. Supreme Court Law Review, 2020, Disponible en SSRN: https://ssrn.com/abstract=3586056
153. Khoo, Deplatforming misogyny (véase la nota 4).
154. S. Dunn y M. Aikenhead, "On the inter- net, nobody knows you are a dog: contested authorship of digital evidence in cases of gender-based violence", Canadian Journal of Law and Tech. (de próxima publicación).
155. UNFPA (2021). Comprehensive Sexuality Education as a GBV prevention strategy.
156. GBV AoR Helpdesk (2021). Learning Series on Technology-Facilitated Gender- based Violence. Learning Brief 2: Strategies and actions for preventing and responding to technology-facilitated GBV.
157. https://asiapacific.unfpa.org/sites/default/ files/pub-pdf/kNOwVAW-data%20Method- ology.pdf
158. Cornell Tech (2021). New project aims to prevent abuse in encrypted communication. Disponible en: https://tech.cornell.edu/ news/preventing_abuse_in_encrypted_ communication/
159. Organizations and advocates such as the Association for Progressive Communications (https://www.apc.org/en), the World Wide Web Foundation (https://webfounda- tion.org/), Derechos Digitales (https://www.derechosdigitales.org/), Internet Democ- racy Project (https://internet-democracy.in/) or Gender IT (https://genderit.org/es).
160. Véase World Wide Web Foundation, Feminist Internet and Craig Walker (2021). Tech Policy Design Lab: Online Gender- Based Violence and Abuse. Disponible en: https://uploads-ssl.webflow.com/61557f76c8a63ae527a819e6/61557f76c8a63a65a6a81adc_OGBV_Report_June2021.pdf

Parte 3

Panorama de las encuestas

para Medir la Prevalencia de la VBG-FT

El siguiente cuadro ofrece una instantánea de la variedad de estudios de prevalencia que se han publicado en relación con la VBG-FT.

Fuente	Ubicación	Término utilizado y definición	Población y tamaño de la muestra	Datos de prevalencia
Economist Intelligence Unit (2021)[161]	51 países con los mayores índices de penetración de Internet en todas las regiones	Violencia en línea contra las mujeres: mujeres con experiencias personales de violencia en línea	4.500 mujeres de 18 a 74 años	38%
African Development Bank Group (2016)[162]	Kenia	Acoso en línea Contactado por impostores en línea, incitación al odio, ciberbullying y troleo en línea	No definido	>33% (acoso en línea) 33% (otras formas de violencia, incluida el discurso de odio, el ciberbullying y troleo)
Plan International (2020)[163]	31 países en todas las regiones	Acoso en línea, "desde amenazas física o sexual, violencia con comentarios racistas y acoso"	14.000 mujeres jóvenes y niñas de 15 a 25 años	58%
The World Wide Web Foundation (2020)[164]	180 países	Abuso en línea, incluyendo mensajes de amenazas, acoso sexual y compartir información privada fotos y vídeos sin permiso	8.109 encuestados (51% mujeres), la mayoría de 15 a 30 años de edad	52% (de mujeres)
Neema Iyer, Bonnita Nyamwire y Sandra Nabulega (2020)[165]	Cinco países africanos (Etiopía, Kenia, Uganda, Senegal y Sudáfrica)	VBG en línea, incluido el acoso sexual, los insultos ofensivos, el acoso y el doxxing.	3.306 mujeres de 18-65 años, que acceden y utilizan Internet al menos una vez por semana	28.2%
Digital Rights Foundation (2017)[166]	Pakistán	Acoso a través de aplicaciones de mensajería	1.400 jóvenes estudiantes (mayores de 18 años) y sus profesoras en 17 universidades de Pakistán	40%

Fuente	Ubicación	Término utilizado y definición	Población y tamaño de la muestra	Datos de prevalencia
F.M. Hassan, F.N. Khalifa, E.D. El Desouky et al. (2020)[167]	Egipto	Violencia cibernética contra mujeres y niñas	356 mujeres adultas (≥18 años) presente sobre la mujer Grupos de Facebook	41,6%
D. Woodlock, K. Bentley, D. Schulze, N. Mahoney, D. Chung y A. Pracilio (2020)[168]	Australia	Acoso y abuso facilitado por la tecnología	442 profesionales en violencia doméstica, sexual y familiar (426 mujeres)	99,3% (de participantes que han trabajado con personas que sufren abuso facilitado por la tecnología)

La prevalencia de formas específicas de VBG-FT también se ha recogido en iniciativas regionales y nacionales de recopilación de datos, el siguiente cuadro indica un breve resumen:

Forma de VBG-FT	Subtipo	Localización y población	Prevalencia o panorama de datos	Fuente
Acoso en línea	**Acoso en línea, a partir de los 15 años**	Unión Europea, mujeres	11%	A. Van der Wilk (2018)[169]
		31 países de todo el mundo, mujeres jóvenes y niñas de 15 a 25 años	58%	Plan International (2020)[170]
	Acoso en línea, lenguaje abusivo e insultante	31 países de todo el mundo, mujeres jóvenes y niñas de 15 a 25 años	59%	Plan International (2020)[171]
	Acoso en línea, amenazas de violencia sexual	31 países de todo el mundo, mujeres jóvenes y niñas de 15 a 25 años	39%	Plan International (2020)[172]
	Acoso en línea, amenazas de violencia física	31 países de todo el mundo, mujeres jóvenes y niñas de 15 a 25 años	21%	Plan International (2020)[173]
Formas sexualizadas de abuso en línea		Estados Unidos, hombres y mujeres	9% de los hombres y 21% de mujeres de 18-29 años (es decir, más del doble)	Centro de Investigación Pew (2017)[174]
		Canadá, estudiantes universitarios, edad promedio 23,79 años y 72% mujeres	El 88% de las mujeres	Lindsey A. Snaychuk y Melanie L. O'Neill (2020)[175]
		31 países de todo el mundo, mujeres jóvenes y niñas de 15 a 25 años	37%	Plan International (2020)[176]

Forma de VBG-FT	Subtipo	Localización y población	Prevalencia o panorama de datos	Fuente
Ciberacoso	**Ciberacoso, después de los 15 años de edad**	Unión Europea, mujeres	5%	A. Van der Wilk (2018)[177]
	Ciberacoso, en el último año	Unión Europea, mujeres	2%	A. Van der Wilk (2018)[178]
		31 países de todo el mundo, mujeres jóvenes y niñas de entre 15 y 25 años	32%	Plan International (2020)[179]
		Senegal, Sudáfrica, Kenia, Uganda y Etiopía, mujeres de 18 a 65 años	26,7%	N. Iyer, B. Nyamwire y S. Nabulega (2020)[180]
Abuso sexual basado en imágenes	**Compartir imágenes de desnudos o de contenido sexual no consensual**	Países de ingresos elevados (estudio de revisión)	1–12%	N. Henry, A. Flynn y A. Powell (2020)[181]
	Amenazas d compartir Imágenes de desnudos o sexuales	Países ingresos elevados (revisión estudio)	1–15%	N. Henry, A. Flynn y A. Powell (2020)[182]
	Estimación de prevalencia global	Revisión sistemática y metaanálisis, principalmente en poblaciones occidentales	9%	U. Patel y R. Roesch (2020)[183]
Experiencias sexuales no deseadas facilitadas por la tecnología	**Que se le pida participar en actividades o comportamientos sexuales no deseadas**	Países Bajos, adultos de 18 a 88 años	4,6% de los hombres, 6,7% de las mujeres	S.E. Baumgartner, P.M. Valkenburg y J. Peter (2010)[184]
	Realizar al menos 1 de 10 comportamientos de victimización sexual	España, adultos	38%	M. Gámez-Guadix, C. Almendros, E. Borrajo y E. Calvete (2015)[185]

Forma de VBG-FT	Subtipo	Localización y población	Prevalencia o panorama de datos	Fuente
Doxxing		Estados Unidos	29%	Amnistía Internacional (2018)[186]
		Ocho países de renta alta	11%	Amnistía Internacional (2018)[187]
VBG-FT directamente relacionada con la trata o con fines de reclutamiento y explotación		Serbia, sobrevivientes de la trata de personas	31%	Andrijana Radoičić (2020)[188]
Suplantación de identidad	**Al menos una amenaza de suplantación**	India, Bangladesh y Pakistán, miembros cisgénero y no cisgénero	15%	N. Sambasivan, A. Batool, N. Ahmed, T. Matthews, K. Thomas, L.S. Gaytán-Lugo, D. Nemer, E. Bursztein, E. Churchill y S. Consolvo (2019)[189]
	Ataques de suplantación de identidad consistentes en la creación de perfiles falsos con la identidad de la persona sobreviviente.	India, Bangladesh y Pakistán, miembros cisgénero y no cisgénero	12%	N. Sambasivan, A. Batool, N. Ahmed, T. Matthews, K. Thomas, L.S. Gaytán-Lugo, D. Nemer, E. Bursztein, E. Churchill y S. Consolvo (2019)[190]
Discurso de odio sexista		Unión Europea	El 3,1% de las denuncias a plataformas de Internet se refieren a discurso de odio sexista.	A. Van der Wilk (2018)[191]
		Malawi, mujeres 15-45 años	46,3%	D.F. Malanga (2020)[192]
Difamación		Estados Unidos, hombres y mujeres adultos	26% des adultes ont vu de fausses informations les concernant publiées en ligne, les différences entre les sexes étant modestes	Pew Research Center (2017)
		Malawi, mujeres 15-45 años	43,3%	D.F. Malanga (2020)[194]

161. Economist Intelligence Unit, Measuring the prevalence of online violence (véase la nota 65).
162. African Development Bank Group (2016). Minding the gaps: identifying strategies to address gender-based cyberviolence in Kenya. Disponible en: https://www.afdb. org/fileadmin/uploads/afdb/Documents/ Generic-Documents/Policy_Brief_on_Gender_Based_Cyber_Violence_in_Kenya. pdf.
163. Plan International, ¿Libres para estar en línea? (véase la nota 6).
164. The World Wide Web Foundation, the online crisis facing women and girls (véase la nota 78).
165. N. Iyer, B. Nyamwire y S. Nabulega (2020) Alternate Realities, Alternate Internets: African Feminist Research for a Feminist Internet, Policy. Disponible en: https://ogbv.pollicy. org/report.pdf
166. Digital Rights Foundation (2017). Measuring Pakistan Women's Experiences of Online Violence. Disponible en: https://digitalrightsfoundation.pk/wp-content/ uploads/2017/05/ Hamara-Internet-On- line-Harassment-Report.pdf.
167. F.M. Hassan, F.N. Khalifa, E.D. El Desouky, M.R. Salem y M.M. Ali, "Cyber violence pattern and related factors: online survey of females in Egypt", Egyptian Journal of Forensic Sciences, vol. 10, nº 6, (2020), https://doi.org/10.1186/s41935-020- 0180-0
168. Woodlock, K. Bentley, D. Schulze, N. Mahoney, D. Chung and A. Pracilio, (2020). Second National Survey of Technology Abuse and Domestic Violence in Australia. WESNET. Disponible en: https://wesnet.org. au/about/research/2ndnatsurvey/
169. Van der Wilk, Cyber violence and hate speech online against women (véase la nota 52).
170. Plan International, ¿Libres para estar en línea? (véase la nota 6).
171. Ibid.
172. Ibid.
173. Ibid.
174. Duggan, Online harassment 2017 (véase la nota 69).
175. Lindsey A. Snaychuk y Melanie L. O'Neill, "Technology-facilitated sexual violence: prevalence, risk, and resiliency in undergraduate students", Journal of Aggression, Maltreatment & Trauma, vol. 29, núm. 8, (2020), pp. 984-999, DOI: 10.1080/10926771.2019.1710636.
176. Plan International, ¿Libre para estar en línea? (véase nota 6).
177. Van der Wilk, Cyber violence and hate speech online against women (véase la nota 52).
178. Ibid.
179. Plan International, ¿Libres para estar en línea? (véase la nota 6).
180. Iyer, Nyamwire y Nabulega, Alternate realities, alternate internets (véase la nota 165).
181. Henry, Flynn y Powell, Technology-facilitated domestic and sexual violence (véase la nota 32).
182. Ibid.
183. U. Patel y R. Roesch, "The prevalence of technology-facilitated sexual violence: a meta-analysis and systematic review", Trauma, Violence, & Abuse, (2020), doi:10.1177/1524838020958057
184. S.E. Baumgartner, P.M. Valkenburg y J. Peter, "Unwanted online sexual solicitation and risky sexual online behavior across the lifespan", Journal of Applied Developmental Psychology, vol. 31, (2010), pp. 439-447.
185. M. Gámez-Guadix, C. Almendros, E. Borrajo y E. Calvete, "Prevalence and association of sexting and online sexual victimization among Spanish adults", Sexuality Research and Social Policy, vol. 12, (2015), pp. 145-154.
186. Amnistía Internacional, Twitter Intoxicado (véase la nota 5).
187. Ibid.
188. Andrijana Radoičić (2020). Behind the screens: Analysis of human trafficking victims abuse in digital surroundings. Disponible en: http://www.atina.org.rs/en/ behind-screens-analysis-human-traffick- ing-victims-abuse-digital-surroundings
189. N. Sambasivan, A. Batool, N. Ahmed, T. Matthews, K. Thomas, LS. Gaytán-Lugo, D. Nemer, E. Bursztein, E. Churchill y S. Consolvo, "They don't leave us alone anywhere we go: gender and digital abuse in South Asia", CHI '19: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, 4-9 de mayo de 2019. Disponible en: https://storage.googleapis. com/pub-tools-public-publication-data/pdf/acf12158ab313c1e9d80b87ede-065254f64ad9a7.pdf
190. Ibid.
191. Van der Wilk, Cyber violence and hate speech online against women (véase la nota 52).
192. Malanga, Tackling gender-based cyber violence (véase la nota 99).
193. Duggan, Online harassment 2017 (véase la nota 69).
194. Malanga, Tackling gender-based cyber violence (véase la nota 99).

Parte 4

Glosario de términos

Definiciones de VBG-FT

Fuente	Plazo	Definición
ACNUDH (A/HRC/38/47, párrafo 23)[195]	**Violencia en línea contra las mujeres**	La violencia de género en línea contra las mujeres, y especialmente contra las mujeres periodistas que utilizan las tecnologías de la información y la comunicación como herramientas para su trabajo, incluye cualquier 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 redes sociales o correo electrónico, dirigida contra una mujer porque es mujer o que la afecta en forma desproporcionada.
A. Flynn, A. Powell y S. Hindes (2021)[196]	**Abuso facilitado por la tecnología (TFA, por sus siglas en inglés)**	El TFA engloba patrones existentes de violencia, acoso y abuso que se extienden y amplifican a través de los medios digitales, así como nuevas formas de abuso, como el Abuso Basado en Imágenes (IBA, por sus siglas en inglés). El TFA es amplio e incluye muchos subtipos de violencia interpersonal y abuso que utilizan tecnologías móviles, en línea y otras tecnologías digitales. Puede incluir el acoso y los comportamientos de vigilancia, el abuso psicológico y emocional (incluidas las amenazas), la violencia sexual y el IBA, así como el acoso sexual. El término también se refiere a veces de manera más amplia a formas de acoso en línea y ciberbullying en general. El TFA se caracteriza por una intersección de las relaciones de poder de género y los daños de base sexual y/o de pareja íntima, ya que puede implicar una extensión digital de los comportamientos de control coercitivo empleados por los perpetradores de la violencia familiar para vigilar, amenazar y restringir a las parejas o exparejas. Además, se entiende que la TFA se dirige con frecuencia a las mujeres y les afecta de manera desproporcionada.
Naciones Unidas[197]	**Violencia en línea y facilitada por las tecnologías de la información y las comunicaciones contra las mujeres y las niñas**	La definición de violencia en línea contra la mujer se aplica a 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 redes sociales o correo electrónico, dirigida contra una mujer porque es mujer o que la afecta en forma desproporcionada.

Fuente	Plazo	Definición
Instituto Europeo de la Igualdad de Género[198]	**Violencia cibernética contra mujeres y niñas**	La violencia de género perpetrada a través de la comunicación electrónica e Internet. Aunque la violencia cibernética puede afectar tanto a mujeres como a hombres, las mujeres y las niñas experimentan formas diferentes y más traumáticas de violencia cibernética. Existen diversas formas de violencia cibernética contra mujeres y niñas, entre las que figuran el ciberacoso, la pornografía no consentida (o «venganza pornográfica»), los insultos y el acoso por motivos de género, la práctica de «tildar de prostituta», la pornografía no solicitada, la «extorsión sexual», las amenazas de violación y de muerte, el «doxing» (reunir y difundir públicamente datos privados de alguien por internet) y la trata de seres humanos facilitada por medios electrónicos. La violencia cibernética no es un fenómeno completamente separado de la violencia en el «mundo real», de hecho, se percibe más adecuadamente como un continuo de la violencia ejercida fuera de internet.
International Centre for Research on Women[199]	**Violencia basada en género facilitada por la tecnología**	La VBG-FT es la acción de una o más personas que perjudica a otras por su identidad sexual o de género o por imponer normas de género perjudiciales. Esta acción se lleva a cabo utilizando Internet y/o la tecnología móvil e incluye el acoso, la intimidación, el acoso sexual, la difamación, el discurso de odio sexista y la explotación.
TEDIC[200]	**Violencia de género digital**	La violencia de género digital (o en línea) se refiere a actos de violencia de género cometidos, instigados o agravados, en parte o totalmente, mediante el uso de tecnologías de la información y la comunicación, plataformas de redes sociales o servicios de correo electrónico. Esta violencia causa daño psicológico y emocional, refuerza prejuicios, daña la reputación, causa pérdidas económicas y plantea barreras a la participación en la vida pública. Además, puede conducir a formas de violencia sexual y otras formas de violencia física."
A. Powell, A.J. Scott y N. Henry (2018)[201]	**Acoso y abuso digital**	Término genérico que hace referencia a una serie de comportamientos interpersonales nocivos experimentados en Internet, así como a través del teléfono móvil y otros dispositivos de comunicación electrónica. Estos comportamientos en línea incluyen comentarios ofensivos e insultos, acoso selectivo, abuso verbal y amenazas, así como acoso y abuso sexual, basado en la sexualidad y el género. El acoso y abuso sexual, por razón de sexo o sexualidad se refiere a comportamientos nocivos y no deseados de naturaleza sexual o dirigidos a una persona por razón de su sexualidad o identidad de género.
Association for Progressive Communications' Women's Rights Programme[202]	**Violencia contra mujeres relacionada con la tecnología**	Actos de violencia de género cometidos, instigados o agravados, en parte o en su totalidad, por el uso de tecnologías de la información y la comunicación, como teléfonos móviles, Internet, plataformas de redes sociales y correo electrónico.
J. Bailey, A. Flynn y N.Henry[203]	**Violencia y abusos facilitados por la tecnología**	Término genérico utilizado para describir el uso de las tecnologías digitales para perpetrar acoso, abuso y violencia interpersonales, como la violencia sexual, la violencia doméstica y familiar, el odio basado en prejuicios y la discriminación en línea.

Formas de VBG-FT y definiciones

A

Abusos financieros por medios electrónicos
El uso de Internet y otras formas de tecnología para ejercer presión financiera sobre un objetivo, normalmente una mujer víctima de malos tratos por parte de su pareja. Esto puede incluir, por ejemplo, la denegación de acceso a cuentas en línea, la manipulación de la información crediticia para crear puntuaciones negativas y el robo de identidad.[223]

Acoso en línea (por razón de género)
El acoso en línea por razón de género es una conducta que implica el uso de la tecnología para contactar, molestar, amenazar o asustar a otra persona mediante comentarios verbales y, a menudo, imágenes inoportunas, ofensivas, degradantes o insultantes, y que es cometida por individuos o grupos de hombres, basándose en el género, la sexualidad o la orientación sexual de la víctima.[239]

Acoso entre plataformas
Acoso coordinado y deliberadamente desplegado contra un objetivo, por un solo acosador o un grupo de acosadores, a través de múltiples espacios en línea, redes sociales y plataformas de comunicación, aprovechando el hecho de que la mayoría de las plataformas sólo moderan el contenido en sus propios sitios.[206]

Amenazas
Una amenaza es "una declaración de intención de causar dolor, lesiones, daños u otra acción hostil" contra una persona objetivo. Esto incluye las amenazas de muerte y las amenazas de violencia física y/o sexual.[251]

Astroturfing o Campañas cordinadas
Difusión o amplificación de contenidos (incluido el abuso) que parecen surgir orgánicamente a nivel popular y difundirse, pero que en realidad están coordinados (a menudo utilizando múltiples cuentas falsas) por un individuo, grupo de interés, partido político u organización.[204]

Avergonzar a las trabajadoras sexuales en línea
Una forma de acoso por razón de género dirigida a menudo a las adolescentes y a las personas LGBTQIA+, que consiste en criticar si no se ajustan a las expectativas sociales en cuanto a comportamiento, apariencia y sexualidad, a menudo arraigadas en las normas de género. Avergonzar a las mujeres trabajadoras sexuales, el acoso, el uso de fotografías no consentidas y la vigilancia sexual a menudo se solapan, amplificando el impacto sobre las víctimas.[247]

B

Bombardeo en Google
Optimización deliberada de información y sitios web maliciosos en línea para que los usuarios vean contenidos difamatorios cuando busquen a una persona.[228]

C

Catfishing
Estafa por Internet en la que el agresor finge ser alguien que no es, creando identidades en línea falsas en las redes sociales -a menudo utilizando fotos de otras personas y desarrollando extensas historias de vida y experiencias, trabajos y amigos falsos- con el objetivo de seducir a

otra persona o hacerle creer que mantiene una relación en línea y utilizarla como medio para pedirle dinero, regalos o imágenes íntimas.[205]

Ciberacoso

Forma grave de persecución ciberobsesional, motivada por el control o la destrucción relacional, que consiste en el uso de la tecnología para acosar y vigilar repetidamente las actividades y comportamientos de alguien en tiempo real o históricamente y que provoca miedo en la persona sobreviviente.[212]

Ciberbullying

Término genérico que hace referencia a un "daño intencionado y provocado infligido mediante el uso de computadores, teléfonos móviles y otros dispositivos electrónicos"[207] normalmente con contenido textual o gráfico y con el objetivo de atemorizar y socavar la autoestima o la reputación de alguien.[208] Este término se utiliza principalmente en relación con niños, niñas y jóvenes.[209]

Contenidos sexuales falsos

Manipulación de imágenes, haciendo que parezca que las personas están participando en una actividad sexual en la que no han participado. Los contenidos sexuales falsos pueden producirse con fines de entretenimiento sexual y lucro, para acosar a las mujeres y causarles daño a propósito. Puede incluir el uso de software para superponer la cara de una persona en una imagen sexual. Las falsificaciones realizadas por la IA son una forma de redes sociales sintéticos.[249]

Cyberflashing

Forma de abuso basado en la imagen por la que una persona envía una imagen no solicitada de sus genitales o material sexualmente explícito a otra persona sin su consentimiento.[210] También conocido como "dick pics", el cyberflashing es una forma de pornografía no deseada que se refiere más ampliamente al "envío de pornografía no solicitada, gifs porno de violaciones violentas o fotografías en las que la imagen de una persona ha sido sexualizada[211]

***Deadnaming* o "usar el nombre muerto"**

Una forma de acoso directo en la que se revela el nombre anterior de la víctima en contra de sus deseos con el fin de perjudicarla. Esta técnica se utiliza con mayor frecuencia para expulsar a miembros de la comunidad LGTBQIA+ que pueden haber cambiado sus nombres de nacimiento por diversas razones, entre ellas para evitar la discriminación profesional y el peligro físico.[214]

Falsificaciones realizadas por la IA o contenidos sintéticos

Imágenes digitales y audio que se alteran o manipulan artificialmente mediante IA y/o aprendizaje profundo para que parezca que alguien hace o dice algo que en realidad no hizo o dijo. Las imágenes o los vídeos pueden editarse para poner a alguien en una posición comprometida o para que haga una declaración controvertida, aunque la persona no haya hecho o dicho realmente lo que se muestra. Cada vez resulta más difícil distinguir el material creado artificialmente de los vídeos y las imágenes reales.[215] Las falsificaciones realizadas por la IA se utilizan cada vez más para crear imágenes sexuales no consentidas que muestran a la persona de forma sexual, por ejemplo, colocando rostros de mujeres en vídeos porno.[216]

Denegación de acceso

Aprovechamiento de las "características de una tecnología o plataforma para perjudicar a una persona, normalmente impidiendo el acceso a herramientas o plataformas digitales esenciales". Hay dos formas principales de denegar el acceso a una plataforma tecnológica: (1) la denuncia masiva o falsa denuncia, que consiste en la acción coordinada de los agresores para denunciar falsamente la cuenta de un objetivo como abusiva o dañina para intentar que se suspenda o se cierre y (2) el bombardeo de mensajes o inundación, que consiste en "inundar" las cuentas de teléfono o correo electrónico de una persona o institución con mensajes no deseados destinados a limitar o bloquear la capacidad de la persona para utilizar esa plataforma.[218]

Difamación
La difamación implica la difusión pública de información exagerada o falsa que dañe la reputación de una persona y que tenga la intención de humillar, amenazar, desacreditar, intimidar o castigar a la víctima y, en particular, a figuras públicas (por ejemplo, funcionarios públicos, activistas y periodistas).[217]

Discurso al odio (sexista o de género)
Cualquier tipo de comunicación verbal, escrita o de comportamiento que ataque o utilice un lenguaje peyorativo o discriminatorio contra una persona o un grupo en función de lo que son, en este caso, en función de su sexo, género, orientación sexual o identidad de género. El discurso de odio sexista y de género en línea, refuerza el sexismo sistémico a la vez que deshumaniza y fomenta la violencia contra las mujeres, las niñas y las personas LGBTQIA+.[226]

Ataques de denegación de servicio (DoS, por sus siglas en inglés)
Ciberataque que provoca la caída temporal o indefinida de un sitio web o una red, o su inoperatividad, al saturar el sistema con datos. Los ataques DoS pueden impedir que las personas accedan a sus propios dispositivos y datos, y pueden poner en peligro la información confidencial almacenada en esos dispositivos. La denegación de servicio distribuida (DDoS) se produce cuando un atacante toma el control de los computadores de varios usuarios para atacar el computador de otro usuario. Esto puede obligar a los computadores secuestrados a enviar grandes cantidades de datos a un sitio web concreto o a enviar spam a direcciones de correo electrónico específicas.[219]

Documentar o difundir agresiones sexuales (vídeos de violaciones)
Grabar y/o difundir imágenes de agresiones sexuales en las redes sociales, a través de texto o en sitios web. Se considera una forma adicional de violencia sexual contra la víctima-sobreviviente.[220] Estos vídeos pueden utilizarse posteriormente para avergonzar o extorsionar a las sobrevivientes, o venderse como pornografía no consentida.[221]

Doxxing* o *doxing
Forma sexista de acoso en línea consistente en la divulgación no consentida de información personal que implica la divulgación pública

de información privada, personal y sensible de una persona, como su domicilio, su dirección de correo electrónico, sus números de teléfono, los datos de contacto de su empleador y de sus familiares, o fotos de sus hijos y del colegio al que asisten, con el fin de hostigarla y causarle daño físico.[222]

E

Experiencias sexuales no deseadas facilitadas por la tecnología
Uso de tecnologías de la comunicación, como teléfonos móviles, correo electrónico, redes sociales, salas de chat o sitios y aplicaciones de citas en línea, para cometer o facilitar agresiones o abusos sexuales.[250]

F

Falsas acusaciones de blasfemia
Las mujeres se enfrentan a amenazas en línea en todo el mundo, pero corren un riesgo único en los países religiosos conservadores, donde la blasfemia es contraria a la ley y los crímenes de honor son una grave amenaza. Acusar a alguien de blasfemia puede convertirse, en sí mismo, en un acto de violencia[224].

Flaming
Publicar o enviar mensajes ofensivos por Internet. Estos mensajes, llamados "flames", pueden publicarse en foros de debate o grupos de noticias en línea, o enviarse por correo electrónico o programas de mensajería instantánea. El ámbito más común en el que tiene lugar el flaming son los foros de debate en línea.[225]

G

***Grooming* (en línea)**
Tipo específico de experiencia sexual facilitada por la tecnología mediante la cual se contacta con niños, niñas y jóvenes a través de las redes sociales u otras plataformas digitales con el fin de agredirlos sexualmente.[229] El reclutamiento de niños, niñas y jóvenes en línea consiste en establecer una relación abusiva en línea con un niño, niña o joven con el fin de llevarlo a situaciones de abuso sexual o trata de menores.[230]

H

Hackear
Uso de la tecnología para obtener acceso ilegal o no autorizado a sistemas o recursos con el fin de atacar, dañar o incriminar a otra persona u organización robando sus datos, obteniendo información personal, alterando o modificando información, violando su privacidad o infectando sus dispositivos con virus.[231]

***Hashtag poisoning* o envenenamiento de etiquetas**
La creación de un hashtag abusivo, o el secuestro de un hashtag existente, que luego se aprovecha como argumento para los ataques de ciberdelincuentes.[232]

I

Abuso basado en la imagen (IBA, por sus siglas en inglés)
Utilización de imágenes para coaccionar, amenazar, acosar, obligar o abusar de una sobreviviente. Incluye una amplia gama de comportamientos que implican tomar, compartir o amenazar con compartir imágenes íntimas sin consentimiento. Estas imágenes pueden ser de naturaleza sexual, en cuyo caso hablamos de "abuso sexual basado en imágenes".[233]

Ataques en la vida real (IRL, por sus siglas en inglés)
Incidentes en los que el abuso en línea se traslada al mundo "real" o ya forma parte de una interacción continua de acoso o violencia de pareja. El troleo IRL también puede significar simplemente intentar infundir miedo haciendo saber a la víctima que el agresor conoce su dirección o lugar de trabajo.[235]

L

Limitar o controlar el uso de la tecnología
Los agresores pueden utilizar la tecnología para ejercer abuso y control sobre la sobreviviente, rastreando, monitoreando o restringiendo sus movimientos, comunicaciones y actividades. Estos comportamientos abusivos van desde obligar a sus parejas a dar sus contraseñas y obtener acceso no autorizado a sus cuentas en línea, hasta limitar su uso de dispositivos tecnológicos. En las relaciones íntimas abusivas, las amenazas a la intimidad en el uso de la tecnología pueden ser precursoras de otras formas de abuso.[236]

M

Mobbing* o *dogpiling
También llamado ciberacoso o acoso en red, consiste en ataques organizados, coordinados y sistemáticos por parte de un grupo de personas contra personas o temas concretos, como los grupos que atacan a feministas o a personas que publican en Internet sobre temas relacionados con la igualdad racial.[237] Las turbas de la indignación o de la vergüenza son una forma de justicia popular centrada en exponer, humillar y castigar públicamente a una persona, a menudo por expresar opiniones sobre temas o ideas políticamente cargados con los que la turba de la indignación no está de acuerdo y/o que se han sacado de contexto para promover una agenda concreta.[238]

P

Persecución ciberobsesional
Búsqueda no deseada de intimidad a través de una invasión reiterada del sentido de intimidad física o simbólica de una persona, utilizando medios digitales o en línea.[213]

R

Reclutamiento
Uso de la tecnología para atraer a posibles víctimas/sobrevivientes a situaciones violentas[240] o para facilitar agresiones físicas o sexuales en persona.[241] Los delincuentes y traficantes pueden utilizar la tecnología para contactar con posibles víctimas a través de publicaciones y anuncios fraudulentos en sitios y aplicaciones de citas, "agencias matrimoniales" o publicar falsas oportunidades de empleo y estudio.[242]

Represalias contra personas que apoyan a sobrevivientes.
Amenazas o acoso a familiares, amigos, empleadores o comunidad de partidarios de una víctima.[243]

S

***Sexting* y *sexting* abusivo**
El sexting es el intercambio electrónico consentido de fotografías de desnudos o de contenido sexual. Sin embargo, es diferente del intercambio no consentido de las mismas imágenes. Aunque el sexting se suele calificar de peligroso, el peligro y la infracción residen en realidad en la violación de la intimidad y el consentimiento que conlleva compartir imágenes sin el consentimiento del sujeto. Por ejemplo, aunque los niños y las niñas adolescentes envían mensajes sexuales en la misma proporción, los niños tienen entre dos y tres veces más probabilidades de compartir las imágenes que les envían.[244]

Sextorsión
Se produce cuando una persona tiene, o dice tener, una imagen sexual de otra persona y la utiliza para coaccionarla a hacer algo que no desea.[245]

Swatting
Realización de una llamada falsa a la policía u otros servicios de emergencia en la que se detalla una amenaza totalmente falsa que tiene lugar en el domicilio o la empresa de una persona, con la intención de enviar una unidad de policía completamente armada (por ejemplo, un equipo SWAT) al domicilio de la persona objetivo. Los

agresores informan de una amenaza o emergencia grave, lo que provoca una respuesta policial que puede incluir el uso de armas y la posibilidad de resultar herido o muerto. El swatting es poco frecuente, pero extremadamente peligroso, y un claro ejemplo de cómo el acoso en línea puede causar daños en la vida real.[248]

T

Troleo de conmoción y dolor
Atacar a las personas sobrevivientes utilizando los nombres y las imágenes de sus seres queridos para crear memes, sitios web, cuentas falsas de Twitter o páginas de Facebook.[246]

Troleo de género
Abuso o acoso en línea por "diversión". Los trolls publican libremente comentarios o mensajes, suben imágenes o vídeos y crean hashtags con el fin de molestar, provocar o incitar a la violencia contra las mujeres y las niñas. Los trolls parecen disfrutar cuando la gente se molesta por lo que publican, y a menudo se desentienden ante las quejas sobre su comportamiento, alegando que todo fue por diversión.[227] Muchos trolls son anónimos y utilizan cuentas falsas.

U

***Upskirting*, *creepshots* y voyerismo digital**
Estas formas de IBA y vigilancia sexual consisten en tomar fotografías o vídeos no consentidos de sobrevivientes, principalmente mujeres y niñas, en lugares públicos como tiendas, baños públicos, vestuarios, aulas o en la calle, pero también en sus propios apartamentos. Pueden consistir en tomar imágenes por debajo del vestido o la falda de una persona (upskirting)[252] , tomar una fotografía sexualmente sugerente de una mujer sin que ésta se dé cuenta (creepshot)[253] o vigilar u observar clandestinamente con el uso de herramientas tecnológicas, y en algunos casos grabar, a otra persona en lo que genéricamente se consideraría un lugar privado (voyerismo digital)[254] .

Z

Zoom-bombing
Se produce cuando las personas se unen a reuniones o encuentros en línea para publicar contenidos racistas, sexistas, pornográficos o antisemitas con el fin de escandalizar y perturbar a los espectadores; es una forma de acoso en red.[255]

Términos relacionados con la tecnología

A

Algoritmo
Un algoritmo es un procedimiento o fórmula para resolver un problema, es decir, una serie de instrucciones que indican a un computador cómo transformar un conjunto de datos en información útil. Los algoritmos se utilizan ampliamente en todas las áreas de la informática. Por ejemplo, cualquier programa informático puede considerarse un algoritmo elaborado.[256]

Aplicación o App
Programas informáticos, generalmente para dispositivos móviles, como teléfonos inteligentes y tabletas, en los que la descarga y la instalación suelen realizarse en el mismo paso, sin que el usuario tenga que hacer nada más, y que pueden eliminarse sin afectar al funcionamiento del dispositivo.[257]

D

Dron
En términos tecnológicos, un dron es una aeronave no tripulada, es decir, un robot volador que puede controlarse a distancia o volar de forma autónoma mediante planes de vuelo controlados por software en sus sistemas integrados, trabajando en conjunción con sensores a bordo y GPS. Los drones se conocen más formalmente como vehículos aéreos no tripulados (UAV, por sus siglas en inglés) o sistemas de aeronaves no tripuladas (UAS, por sus siglas en inglés). Los drones se utilizan actualmente en una amplia gama de funciones civiles que van desde la búsqueda y rescate, la vigilancia, la supervisión del tráfico, el monitoreo meteorológico y la extinción de incendios, hasta los drones personales y la fotografía empresarial basada en drones, así como la videografía, la agricultura e incluso entregas domiciliarias.[261]

E

Empresas privadas de tecnología, o empresas tecnológicas[265]
Las empresas tecnológicas privadas engloban un amplio abanico de organizaciones, entre las que se incluyen las siguientes:

- Proveedores de servicios de Internet designados: entidades que permiten a los usuarios finales acceder a materiales en línea, y proveedores de servicios de Internet, que son las entidades que prestan servicios de navegación por Internet, incluidos, entre otros, Google, Safari e Internet Explorer;
- Proveedores de servicios de redes sociales: entidades que prestan servicios que conectan a dos usuarios finales a través de medios en línea, incluidos, entre otros, Facebook, LinkedIn e Instagram;
- Proveedores de servicios electrónicos: entidades que permiten a los usuarios finales comunicarse entre sí (por ejemplo, Outlook y los servicios de chat de juegos);
- Proveedores de servicios de distribución de aplicaciones: entidades que proporcionan acceso a servicios de aplicaciones, como Google (a través de Google PlayStore) y Apple (a través de IOS App Store);
- Proveedores de servicios de hosting: entidades que permiten el hosting de materiales almacenados proporcionados en servicios de redes sociales, servicios electrónicos pertinentes o servicios de Internet designados,


1458
Options
Clear
SAMSUNG
OK

incluidos, entre otros, Apple y Microsoft, cada uno a través de su prestación de servicios en la nube;

- Empresas de desarrollo de hardware: entidades que crean, desarrollan y/o mantienen equipos tecnológicos, activos físicos y otros artículos tangibles;;
- Empresas de desarrollo de software: entidades que crean, diseñan, desarrollan y mantienen programas, aplicaciones, marcos u otros componentes de software.

G

GPS y seguimiento por GPS

El seguimiento por GPS es la vigilancia de la localización mediante el uso del Sistema de Posicionamiento Global (GPS, por sus siglas en inglés) para rastrear a distancia la ubicación de una entidad u objeto. El GPS es una "constelación" de 24 satélites bien espaciados que orbitan alrededor de la Tierra y permiten a personas con receptores en tierra (o dispositivos de seguimiento GPS) determinar su ubicación geográfica. La precisión de la localización oscila entre 10 y 100 metros para la mayoría de los equipos. En la actualidad, los equipos GPS están integrados en teléfonos inteligentes, tabletas y dispositivos de navegación GPS. Los dispositivos GPS de los teléfonos inteligentes y otros dispositivos móviles se utilizan a menudo para localizar a los empleados, por ejemplo. Los defensores de la privacidad advierten de que esta tecnología también puede permitir a empresas, gobiernos, hackers y ciberacosadores rastrear a los usuarios a través de sus dispositivos móviles.[262]

I

Inteligencia Artificial (IA)

En su forma más simple, la inteligencia artificial es un campo que combina la informática y conjuntos de datos robustos para permitir la resolución de problemas. También engloba los subcampos del aprendizaje automático y el aprendizaje profundo, que se mencionan con frecuencia junto con la inteligencia artificial. La inteligencia artificial busca crear sistemas expertos que hagan predicciones o clasificaciones basadas en datos de entrada y aprovecha las computadoras y máquinas para imitar las capacidades de resolución de problemas y toma de decisiones de la mente humana258.

P

Plataforma digital

Las plataformas digitales son empresas en línea que facilitan las interacciones comerciales y los intercambios de información, bienes o servicios entre productores y consumidores, así como entre la comunidad que interactúa con dicha plataforma. Las plataformas digitales pueden ser plataformas de redes sociales (Facebook, Twitter y LinkedIn), plataformas de conocimiento (Yahoo Respuestas y Google Scholar), plataformas para compartir medios (Spotify, YouTube y Netflix) o plataformas orientadas a los servicios (Airbnb, Amazon y Uber).[259]

Plataforma en línea

Una plataforma en línea es un servicio digital que facilita las interacciones entre dos o más grupos de usuarios (ya sean empresas o particulares) distintos pero interdependientes que interactúan a través del servicio por Internet. El término "plataforma en línea" se ha utilizado para describir una serie de servicios disponibles en Internet, incluidos los mercados, los motores de búsqueda, las redes sociales, los puntos de venta de contenidos creativos, las tiendas de aplicaciones, los servicios de comunicaciones, los sistemas de pago, los servicios que comprenden la llamada economía "colaborativa" o "gig", y muchos más[264].

R

Redes sociales

Las redes sociales son un término colectivo para referirse a sitios web y aplicaciones que se centran en la comunicación a través de Internet, los aportes de la comunidad, la interacción, el intercambio de contenidos y la colaboración. Foros, microblogging, redes sociales, marcadores sociales, curación de contenidos en redes y wikis son algunos de los distintos tipos de redes sociales que permiten una rápida comunicación electrónica de contenidos a los usuarios. El contenido incluye información personal, documentos, vídeos y fotos. Los usuarios se conectan a las redes sociales a través de un computador, una tableta o un teléfono inteligente mediante programas o aplicaciones web. Las plataformas de redes sociales más utilizadas son Facebook, YouTube, WhatsApp, Facebook Messenger, Instagram y TikTok.[266]

S

Spyware

El spyware es un tipo de software malicioso que se instala en un dispositivo informático sin el conocimiento del usuario final. Invade el dispositivo, roba información sensible y datos de uso de Internet y los transmite a empresas privadas, empresas de datos o usuarios externos. Una vez instalado, monitorea la actividad en Internet, rastrea las credenciales de inicio de sesión y espía información sensible.

Los programas espía también pueden utilizarse para rastrear la ubicación de una persona, como es el caso de los **stalkerware**. Los cónyuges, las parejas íntimas, las exparejas e incluso los padres o familiares suelen instalar estos programas en los teléfonos móviles. Este tipo de software espía puede rastrear la ubicación física de la persona sobreviviente e interceptar sus correos electrónicos y mensajes de texto, espiar sus llamadas telefónicas y grabar conversaciones, y acceder a datos personales, como fotos y vídeos

T

Tecnologías de la información y la comunicación

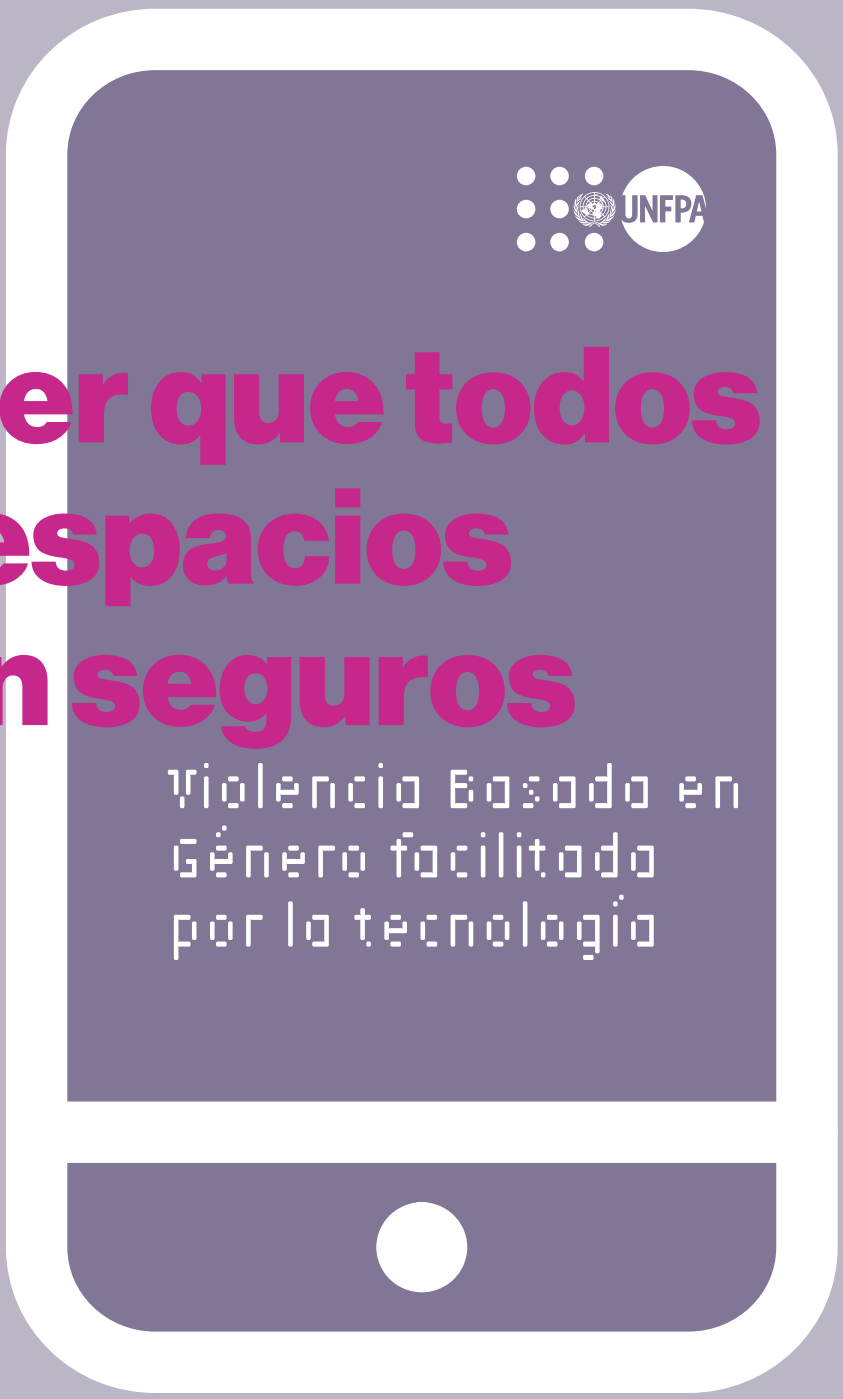
Conjunto diverso de herramientas y recursos tecnológicos utilizados para transmitir, almacenar, crear, compartir o cambiar información. Estas herramientas y recursos tecnológicos incluyen computadores, Internet (sitios web, blogs y correos electrónicos), tecnologías de difusión en directo (radio, televisión y webcasting), tecnologías de difusión grabada (podcasting, reproductores de audio y vídeo y dispositivos de almacenamiento) y telefonía (por ejemplo, fija o móvil, por satélite y videollamadas).[263]

Tecnologías digitales

Las tecnologías digitales son herramientas, sistemas, dispositivos y recursos electrónicos que generan, almacenan o procesan datos. Incluyen la infraestructura, los dispositivos, los medios de comunicación, los servicios en línea y las plataformas que utilizamos para la comunicación, la formación, la documentación, la creación de redes/relaciones y las necesidades de identidad.[260]

195. OHCHR (2018). Report of the Special Rapporteur on violence against women (véase la nota 11).
196. Flynn, Powell y Hindes, Technology-facilitated abuse (véase la nota 3).
197. Consejo de Derechos Humanos de las Naciones Unidas. Informe de la Relatora Especial Dubravka Šimonović (18 de junio de 2018 Informe de la Relatora Especial sobre la violencia contra la mujer, sus causas y consecuencias acerca de la violencia en línea contra las mujeres y las niñas desde la perspectiva de los derechos humanos. UN Doc A/HRC/38/47.
198. https://eige.europa.eu/publications/cyber- violence-against-women-and-girls
199. L. Hinson, J. Mueller, L. O'Brien-Milne y N. Wandera (2018). Technology-facilitated Gender-based Violence: What Is It, and How Do We Measure it? (Washington D.C.: Inter- national Center for Research on Women). Disponible en: https://www.svri.org/sites/ default/files/attachments/2018-07-24/ ICRW_VBG-FTMarketing_Brief_v8-Web.pdf
200. https://violenciadigital.tedic.org/index-Eng. html#violencia
201. Anastasia Powell, Adrian J. Scott y Nicola Henry, "Digital harassment and abuse: experiences of sexuality and gender minority adults", European Journal of Criminology, vol. 17, núm. 2, (2018), pp. 199–223. https://journals.sagepub.com/ doi/full/10.1177/1477370818788006
202. Association for Progressive Communications (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. Disponible en: https://www. apc.org/sites/default/files/APCSubmis- sion_UNSR_VAW_GBV_0_0.pdf
203. J. Bailey, A. Flynn y N. Henry, "Prelims", en The Emerald International Handbook of Technology Facilitated Violence and Abuse, J. Bailey, A. Flynn y N. Henry, eds. (Bing- ley, Emerald Publishing Limited, 2021) pp. i-xxiv. https://doi.org/10.1108/978-1- 83982-848-520211059
204. Penn América, Manual de campo del acoso en línea. Disponible en: https://onlinehar- assmentfieldmanual.pen.org/defining-on- line-harassment-a-glossary-of-terms/
205. eSafety Commission Australia. Catfishing. Disponible en: https://www.esafety.gov.au/ young-people/catfishing
206. Penn América, Manual de campo del acoso en línea.
207. Cyberbullying Research Centre. What is cyberbullying? Disponible en: https://cyber- bullying.org/what-is-cyberbullying
208. Van der Wilk, Cyber violence and hate speech online against women (véase la nota 52).
209. Penn America, Manual de campo del acoso en línea.
210. Flynn, Powell y Hindes, Technology-facilitated abuse (véase la nota 3).
211. Women's Media Centre. WMC Speech Project: Online Abuse 101. Disponible en: https://womensmediacenter.com/speech-project/online-abuse-101
212. VAW Learning Network, Technology-related violence against women (véase la nota 20) Henry y Powell, Technology-facilitated sexual violence (véase la nota 22).
213. Ibíd.
214. Women's Media Centre, WMC Speech Project.
215. John R. Allen and Darrell M. West (2020). The Brookings glossary of AI and emerging technologies. Disponible en: https://www.brookings.edu/blog/tech- tank/2020/07/13/the-brookings-glossa- ry-of-ai-and-emerging-technologies/
216. Flynn, Powell y Hindes, Technology-facilitated abuse (véase la nota 3).
217. Douglas, Doxing: a conceptual analysis (véase la nota 40). Dunn, Technology-facilitated gender-based violence: an overview (véase la nota 24).
218. Penn América, Manual de campo del acoso en línea.
219. Ibid.
220. GBV AoR Helpdesk, Learning Series on Technology-Facilitated Gender-Based Violence (véase la nota 100).
221. 221 Women's Media Centre, WMC Speech Project.
222. MacAllister, The doxing dilemma (véase la nota 38). Douglas, Doxing: a conceptual analysis (véase la nota 40).
223. Women's Media Centre, WMC Speech Project.
224. Ibíd.
225. https://techterms.com/definition/flaming
226. ONU, Estrategia y Plan de Acción de las Naciones Unidas para la lucha contra el discurso de odio (véase la nota 58).
227. Safety Commission Australia. Online abuse targeting women. Disponible en: https://www.esafety.gov.au/women/online-abuse-targeting-women
228. Women's Media Centre, WMC Speech Project.
229. Craven, Brown y Gilchrist, Sexual grooming of children (véase la nota 36).
230. Van der Wilk, Cyber violence and hate speech online against women (véase la nota 52).
231. Penn America, Manual de campo del acoso en línea. VAW Learning Network, Technology-related violence against women (véase la nota 20).
232. Penn America, Manual de campo del acoso en línea.
233. Flynn, Powell y Hindes, Technology-facilitated abuse (véase la nota 3). McGlynn, Rackley y Houghton, Beyond revenge porn (véase la nota 9).
234. Van der Wilk, Cyber violence and hate speech online against women (véase la nota 52).
235. Women's Media Centre, WMC Speech Project.
236. Levy y Schneier, Privacy threats in intimate relationships (véase la nota 62).
237. GBV AoR Helpdesk, Learning Series on Technology-Facilitated Gender-Based Violence (véase la nota 100).
238. Penn America, Manual de campo contra el acoso en línea.
239. VAW Learning Network, Technology-related violence against women (véase la nota 20). Henry y Powell, Technology-facilitated sexual violence (véase la nota 22). Flynn, Powell y Hindes, Technology-facilitated abuse (véase la nota 3).
240. VAW Learning Network, Technology-related violence against women (véase la nota 20).
241. Fascendini y Fialová, Voices from digital spaces (véase la nota 14).
242. APC, How technology is being used to perpetrate violence against women (véase la nota 48).
243. Women's Media Centre, WMC Speech Project.
244. Ibid.
245. Dunn, Technology-facilitated gender-based violence: an overview (véase la nota 24).
246. Women's Media Centre, WMC Speech Project.
247. Ibíd.
248. Women's Media Centre, WMC Speech Project. Penn America, Manual de campo contra el acoso en línea.
249. Dunn, Technology-facilitated gender-based violence: an overview (véase la nota 24).
250. Henry, Flynn, and Powell, Technology-facilitated domestic and sexual violence (véase la nota 32).
251. Penn America, Manual de campo del acoso en línea.
252. Flynn, Powell y Hindes, Technology-faciliitated abuse (véase la nota 3).
253. Lexico. https://www.lexico.com/definition/ creepshot
254. Clough,J (2015). Harassment, en Principles of Cybercrime (pp. 417 - 453). Cambridge: Cambridge University Press. doi:10.1017/ CBO9781139540803.013.

255. Dunn, Technology-facilitated gender-based violence: an overview (véase la nota 24).
256. The Conversation (2020). What is an algorithm? How computers know what to do with data. Disponible en: https:// theconversa- tion.com/what-is-an-algorithm-how-com- puters-know-what-to-do-with-data-146665
257. Techopedia (2012). App. Disponible en: https://www.techopedia.com/definition/28104/app
258. IBM (2020). Inteligencia Artificial (IA). Disponible en: https://www.ibm.com/cloud/learn/ what-is-artificial-intelligence
259. BMC blogs (2020). Digital Platforms: A Brief Introduction. Disponible en: https://www.bmc. com/blogs/digital-platforms/#
260. GBV AoR Helpdesk, Learning Series on Technology-Facilitated Gender-Based Violence (véase la nota 100).
261. IoT Agenda (2019). Drone (UAV). (vehículo aéreo no tripulado). Disponible en: https://internetofthingsagenda.techtar- get.com/definition/drone
262. WhatIs.com (2014). GPS tracking. Disponible en: https://whatis.techtarget.com/defi- nition/GPS-tracking
263. UNESCO Institute for Statistics. Glossary: Information and communication technologies (ICT). Disponible en: http://uis.unesco. org/en/glossary
264. OECD (2019). An Introduction to Online Platforms and Their Role in the Digital Transformation. Disponible en: https:// www.oecd-ilibrary.org/science-and-tech nology/an-introduction-to-online-plat forms-and-their-role-in-the-digital-trans formation_53e5f593-es
265. Online Safety Act 2021 (Cth). No. 76, 2021. (Austl.)
266. GBV AoR Helpdesk, Learning Series on Technology-Facilitated Gender-Based Violence (véase la nota 108).
267. TechTarget (2021). Spyware. Disponible en: https://searchsecurity.techtarget.com/defi nition/spyware



Hacer que todos los espacios sean seguros

Violencia Basada en Género facilitada por la tecnología

Fondo de Población de las Naciones Unidas
605 Third Avenue, New York, NY 10158
1-212-297-5000 / www.unfpa.org / @UNFPA